Zapytanie o informację

(RFI)

Warszawa lipiec 2018

I. Przedmiot i cel Zapytania o informację

1. Zakład Ubezpieczeń Społecznych rozważa dokonania zakupu oprogramowania **Zakup licencji VMware do wirtualizacji zasobów serwerowych albo oprogramowania równoważnego.**
2. Celem niniejszego zapytania o informację jest pozyskanie przez Zakład Ubezpieczeń Społecznych od podmiotów zajmujących się profesjonalnie określonym zakresem, danych dotyczących szacunkowego kosztu realizacji.

II. Ogólne informacje o charakterze formalnym

1. Niniejsze Zapytanie o informację nie stanowi oferty zawarcia umowy w rozumieniu przepisów *ustawy z dnia 23 kwietnia 1964 r.- Kodeks cywilny*. Udzielenie odpowiedzi na niniejsze Zapytanie o informację nie będzie uprawniało do występowania z jakimikolwiek roszczeniami w stosunku do Zakładu Ubezpieczeń Społecznych.
2. Niniejsze Zapytanie o informację nie jest elementem jakiegokolwiek postępowania o udzielenie zamówienia, w rozumieniu *ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych*, jak również nie jest elementem jakiegokolwiek procesu zakupowego prowadzonego w oparciu o wewnętrzne regulacje Zakładu Ubezpieczeń Społecznych.
3. Złożenie odpowiedzi na niniejsze Zapytanie o informację jest jednoznaczne z wyrażeniem zgody przez podmiot składający taką odpowiedź na nieodpłatne wykorzystanie przez Zakład Ubezpieczeń Społecznych wszystkich lub części przekazanych informacji.

III. Termin i sposób złożenia odpowiedzi na Zapytanie o informację

1. Odpowiedź na Zapytanie o informację należy przygotować w oparciu o formularz stanowiący **Załącznik nr 2** do Zapytania o informację.
2. W przypadku, gdy informacje zawarte w odpowiedzi na Zapytanie o informację stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, podmiot składający taką odpowiedź winien to wyraźnie zastrzec w odpowiedzi. Brak przedmiotowego zastrzeżenia, Zakład Ubezpieczeń Społecznych będzie traktował przekazane informacje jako informacje, które nie stanowią tajemnicy przedsiębiorstwa.
3. **W przypadku zaproponowania rozwiązania równoważnego, należy przedstawić dodatkowe informacje tj.: nazwa oprogramowania, producenta, sposób licencjonowania/subskrypcji.**
4. Odpowiedź na Zapytanie o informację należy przesłać w terminie **do 9 lipca 2018 r. do godziny 12:00 na adres e-mail: rfi-wirtualizacja@zus.pl**

I. W ramach realizacji przedmiotu zamówienia Wykonawca:

1. Dostarczy licencje na oprogramowanie VMware lub równoważne:
   a. vSphere v.6 w wersji Standard w ilości **80 szt.**
   b. vSphere v.6 w wersji Enterprise Plus w ilości **546 szt.**
   c. vSphere Remote Office Branch Office Advanced w ilości **pozwalającej na utworzenie maksymalnie 20 maszyn wirtualnych w każdym z 44 ośrodków przetwarzania Zamawiającego**. (44 ośrodki przetwarzania, w każdym 2 serwery po 2 procesory 10-korowe).
   d. vCenter Server w wersji Standard w ilości **8 szt.**
   e. NSX Data Center w wersji Enterprise Plus w ilości **4 szt.**
   f. SRM w wersji Enterprise w ilości **50 szt.**
2. Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta oprogramowania będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę.
3. Opis warunków równoważności dla oprogramowania VMware znajduje się w **Załączniku nr 1**.

II. Warunki świadczenia wsparcia na oprogramowanie

1. Zgłoszenia awarii oprogramowanie będą dokonywane przez 24 godziny, 7 dni w tygodniu, 365 dni w roku.
2. Wymagane jest, aby wysyłanie zgłoszeń serwisowych do Producenta oprogramowania było zapewnione z poziomu portalu użytkownika, służącego również do zarządzania kluczami licencyjnymi do posiadanego oprogramowania do wirtualizacji dostarczonego w ramach tego zamówienia.

III. Odbiór przedmiotu zamówienia.

1. Wykonawca w ciągu 3 dni roboczych od podpisania Umowy przekaże klucze licencyjne na wskazany przez Zamawiającego w dniu podpisania Umowy adres poczty elektronicznej.

Załącznik nr 1 – Opis przedmiotu zamówienia

1. Warunki równoważności dla licencji VMware vSphere w wersji Standard

Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:

- Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego
- Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows XP, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, SLES 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, REHL Atomie 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, 05/2 Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin
- Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych
- Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP made w Windows 7, a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej
- Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji
- Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
- Oprogramowanie do wirtualizacji musi zapewnić możliwość o wykonywania kopi migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez

przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej

- Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP
- Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
- System musi mieć możliwość uruchamiania fizycznych serwerów z przygotowanego obrazu poprzez protokół PXE
- System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych
- System 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 ethernet'owego w razie awarii karty sieciowej
- Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN)
- Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
- Rozwiązanie musi umożliwiać wykorzystanie technologii 1O GbE, w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
- Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania
- Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut
- Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switch'y) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją
- Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi
- Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak, by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury
- Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych

- Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania
- Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn
- Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
- Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana
- Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB
- Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
- Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
- System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
- Wirtualizator musi wspierać TPM 2.0 oznacza to m. in. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego
- Wirtualizator musi mieć włączenia funkcji "Microsoft virtualization-based security", tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows 10 oraz Windows Server 2016
- System musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
- Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że z punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym, wszystkie standardowe funkcjonalności wirtualizatora, tj. wysoka dostępność, czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi, działa prawidłowo.
- Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora

- Wirtualizatora musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego - następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji
- Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów
- Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K

Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Zamawiający wymaga, aby w przypadku wystąpienia problemów, wysyłanie zgłoszeń serwisowych do Producenta było zapewnione z poziomu portalu użytkownika, służącego do zarządzania kluczami licencyjnymi do posiadanego oprogramowania do wirtualizacji.

Poziomy zgłoszeń L1, L2, L3,
L1 - przyjęcie zgłoszenia i wyszukanie w "bazie wiedzy" czy problem jest powtarzalny i czy nie został już zgłoszony w przeszłości przez któregoś z użytkowników , jeżeli tak jest do użytkownika wysyłana jest informacja z rozwiązaniem problemu,
L2 - dalsza analiza problemu i próba jego odtworzenia. Jeżeli w wyniku analizy okaże się, że problem występuje na poziomie kodu źródłowego oprogramowania, wówczas trafia on na poziom L3,
L3 - opracowywanie poprawek na poziomie kodu źródłowego: patch'y, update'ów, bug-fix'ów, itp.

2. Warunki równoważności dla oprogramowania vSphere w wersji Enterprise Plus

Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:

- Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego
- Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows XP, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10,SLES 9, SLES 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, REHL Atomie 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, 05/2

Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux, CoreOS, NeoKylin

- Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych
- Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7, a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej
- Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji
- Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej
- Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP
- Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
- System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE
- System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych
- System 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 ethernet'owego w razie awarii karty sieciowej
- Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN)
- Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
- Rozwiązanie musi umożliwiać wykorzystanie technologii 1O GbE, w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek

- Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
- Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej, w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania
- Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut
- Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switch'y) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi
- Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury
- Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych
- Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania
- Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn
- Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
- Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana
- Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB
- Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
- Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
- Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (automatyzacja) oraz wirtualizacji sieci (SON) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny

kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe)

- System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
- Wirtualizator musi wspierać TPM 2.0 oznacza to m. in. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego
- Wirtualizator musi mieć włączenia funkcji "Microsoft virtualization-based security", tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows 10 oraz Windows Server 2016
- System musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
- Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność, czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizoatora
- Wirtualizatora musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego - następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji
- Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów
- Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K
- Rozwiązanie wirtualizatora musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza, to, że jeśli serwer fizyczny posiad funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizatora na podstawie tych danych, wirtualizator jest w stanie, proaktywnie przenieść wszystkie maszyny wirtualne na inne prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego
- Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej
- Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizującego, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym
- Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna

musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją

- Przełącznik rozproszony musi współpracować z protokołem NetFlow
- Platforma wirtualizacji powinna w ramach przełącznika sieciowego musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych
- Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port
- Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii, a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej
- System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych
- 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
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych platformy wirtualnej
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy różnymi Centralnymi Konsolami Zarządzającymi platformy wirtualnej na daleką odległość min. 300 km
- Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych
- Rozwiązanie powinno posiadać proaktywnie działający mechanizm, który zmigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii
- System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn
- System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką
- System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami 1/0 na mniej obciążone
- Rozwiązanie jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy
- System musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervizor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany)

- System musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach
- System musi umożliwiać instalowanie uruchamianie i zarządzanie aplikacjami „Big Data" oraz „Hadoop" z poziomu platformy wirtualizującej
- Platforma musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU do maszyn wirtualnych
- Wirtualizator musi wspierać tzw. rozwiązanie trwałej, nieulotnej pamięć (Persistent Memory) zbliżonej do szybkości pamięci DRAM. W ten sposób wirtualizator może udostępnić dla maszyn wirtualnych dyski, które wspierają taką funkcjonalność - ultraszybką pamięć masową zbliżoną do pamięci DRAM
- Wirtualizator musi wspierać protokół Remote Direct memory Access (ROMA) poprzez konwergentny Ethernet, lub RoCE ("rocky") v2, Fiber Channel over Ethernet (FCoE) adapter, i iSCSI rozszerzenie dla ROMA (iSER). Dzięki temu maszyny wirtualne można skonfigurować z wykorzystaniem protokołu ROMA

Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Zamawiający wymaga, aby w przypadku wystąpienia problemów, wysyłanie zgłoszeń serwisowych do Producenta było zapewnione z poziomu portalu użytkownika, służącego do zarządzania kluczami licencyjnymi do posiadanego oprogramowania do wirtualizacji.

Poziomy zgłoszeń L1, L2, L3,
L1 - przyjęcie zgłoszenia i wyszukanie w "bazie wiedzy" czy problem jest powtarzalny i czy nie został już zgłoszony w przeszłości przez któregoś z użytkowników, jeżeli tak jest do użytkownika wysyłana jest informacja z rozwiązaniem problemu,
L2 - dalsza analiza problemu i próba jego odtworzenia. Jeżeli w wyniku analizy okaże się, że problem występuje na poziomie kodu źródłowego oprogramowania, wówczas trafia on na poziom L3,
L3 - opracowywanie poprawek na poziomie kodu źródłowego: patch'y, update'ów, bug-fix'ów, itp.

3. Warunki równoważności dla oprogramowania VMware vCenter w wersji Standard

- Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna działać, jako aplikacja na maszynie wirtualnej, jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance
- 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 HTMLS
- 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
- Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną
- Rozwiązanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo musi być możliwość ustawienia harmonogramu wykonywania kopii zapasowej

- 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 HTMLS

Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Zamawiający wymaga, aby w przypadku wystąpienia problemów, wysyłanie zgłoszeń serwisowych do Producenta było zapewnione z poziomu portalu użytkownika, służącego do zarządzania kluczami licencyjnymi do posiadanego oprogramowania do wirtualizacji.

Poziomy zgłoszeń L1, L2, L3,
L1 - przyjęcie zgłoszenia i wyszukanie w "bazie wiedzy" czy problem jest powtarzalny i czy nie został już zgłoszony w przeszłości przez któregoś z użytkowników, jeżeli tak jest do użytkownika wysyłana jest informacja z rozwiązaniem problemu,
L2 - dalsza analiza problemu i próba jego odtworzenia. Jeżeli w wyniku analizy okaże się, że problem występuje na poziomie kodu źródłowego oprogramowania, wówczas trafia on na poziom L3,
L3 - opracowywanie poprawek na poziomie kodu źródłowego: patch'y, update'ów, bug-fix'ów, itp.

4. Warunki równoważności dla oprogramowania VMware NSX Data Center w wersji Enterprise Plus

- Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne
- Oferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych
- Oferowane rozwiązanie realizujące usługi wirtualnych sieci musi być zarządzane przez narzędzie zarządzające warstwą wirtualną serwerów. Wyklucza się używanie skryptów lub plugin'ów nie wspieranych przez dostawcę platformy wirtualizatora serwerów
- Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego przełącznika instalowanego w jądrze wirtualizatora serwerów (Hypervisor), umożliwiający tworzenie logicznych segmentów sieci L2. Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta wirtualizatora serwerów
- Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego routera instalowanego w jądrze wirtualizatora serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska maszyn wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników
- Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN
- Oferowane oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zwirtualizowanego opartego o technologię VXLAN oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów
- Oferowane oprogramowanie musi zapewnić funkcjonalność wirtualnego routera wspierającego protokoły OSPF i BGP. Routing statyczny oraz BGP musi być możliwy poprzez tunel GRE

- Rozwiązanie musi posiadać funkcję łączenia/bridge segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie wirtualnej bramy/bridge
- Rozwiązanie musi umożliwiać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT), jak i przychodzącego (DNAT)
- Rozwiązanie musi posiadać funkcję serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego
- Oferowane rozwiązanie musi posiadać pełną wymaganą funkcjonalność zarówno funkcji bezpieczeństwa oraz funkcji sieciowych w ramach jednego produktu i być gotowe do instalacji i konfiguracji z wykorzystaniem GUI
- Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs, tj. API
- Oprogramowanie do wirtualizacji sieci (SDN) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji serwerów (Hypervisor) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe)
- Zmiana konfiguracji sieciowej musi odbywać się poprzez narzędzia zarządzające dostępne dla środowiska wirtualizacyjnego serwerów
- Aktualizacje oprogramowania powinny odbywać się poprzez zintegrowany portal służący do ich planowania i uruchamiania. Portal musi umożliwiać przegląd wszystkich elementów systemu pod kątem ich aktualnej oraz przygotowanej do aktualizacji wersji. Portal musi oferować wskaźniki postępu aktualizacji, umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia konsystencji działania systemu przed oraz po aktualizacji
- Oprogramowanie powinno zapewniać wsparcie dla wykorzystania plików danych JSON oraz XML
- Oferowane oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie hypervisora/wirtulanego interfejsu sieciowego (vNIC), dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych przełączników lub firewall'i
- Rozwiązania musi posiadać funkcję rozproszonego, stanowego firewall'a instalowanego w/na poziomie jądra wirtualizatora (Hypervisor) serwerów umożliwiający tworzenie polityk bezpieczeństwa w warstwach 2-4 modelu OSI. Nie dopuszcza się stosowania filtracji typu "reflexive". Możliwość definiowania reguł dla warstwy 7 modelu OSI dla wybranych aplikacji w celu zapewnienia kontroli przepływu danych oraz planowania mikrosegmentacji
- Musi zostać zapewniona możliwość tworzenia reguł firewall'a w trybie stateless dla różnych grup wirtualnych maszyn
- Możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i na tym samym fizycznym serwerze
- Rozwiązanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł polityk bezpieczeństwa: Wymagane min.: nazwa maszyny wirtualnej, nazwa switcha wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
- Oferowane rozwiązanie realizujące usługę rozproszonego firewall'a musi być zarządzane przez narzędzie zarządzające warstwą wirtualną serwerów. Wyklucza się używanie skryptów lub plugin'ów nie wspieranych przez dostawcę platformy wirtualizatora serwerów
- Rozwiązanie musi zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do wirtualnej maszyny po zmianie jej adresu IP

- Rozwiązanie powinno oferować w ramach platformy, funkcjonalność bezpiecznego, zdalnego i szyfrowanego dostępu użytkowników dla minimum następujących systemów operacyjnych: Windows 8, Mac OS oraz Linux przy użyciu technologii SSL VPN
- Rozwiązanie powinno oferować w ramach platformy, możliwość terminowania tuneli IPSeC site-to-site z metodą autentykacji współdzielonego klucza (pre shared key) lub certyfikatu
- Rozwiązanie powinno umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall warstwy 7, m.in. Integracja z systemem do zarządzania Next Generation Firewall
- Rozwiązanie musi umożliwiać przekierowanie wybranego ruchu L2 do rozwiązania firm trzecich z obszaru bezpieczeństwa
- Oferowane oprogramowanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu tj. load balancing działającą do warstwy 7 modelu ISO OSI
- Rozwiązanie musi zapewniać następujące mechanizmy przywiązania sesji: adres źródłowy, cookie, SSL ID oraz JSessionlD
- W ramach inspekcji warstwy 7 rozwiązanie musi oferować funkcję blokowania modyfikacji URL
- Rozwiązanie musi oferować możliwość wstrzykiwania nagłówka XFF (X-Fowarder-For)
- Funkcja Wirtualny Load Balancer musi być realizowana i w pełni zintegrowana z platformą do wirtualizacji sieci
- Rozwiązanie typu Identity Firewall musi zapewniać integrację z Active Direcory z obsługą selektywnej synchronizacji
- Rozwiązanie powinno posiadać funkcję łączenia/bridge segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie fizycznego przełącznika firm trzecich
- Rozwiązanie musi zapewniać mechanizm wspomagający planowanie tworzenia grup oraz polityk bezpieczeństwa
- Rozwiązanie musi oferować funkcjonalność typu Identity Firewall umożliwiające obsługę sesji użytkowników na pulpitach wirtualnych (VDI) oraz serwerach aplikacji (RDSH) współdzielących pojedynczy adres IP
- Rozwiązanie musi oferować funkcjonalność identyfikacji aplikacji, np. MySQL, http, DNS, DHCP, Active Directory, TLS, itp. na poziomie sieciowym OSI (warstwa 5-7), a następnie móc wykorzystać tą informację w rozproszonym firewall w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji
- Rozwiązanie musi mieć możliwość analizowania przepływów sieciowych (w tym IPFIX) opartych o wirtualizację VMware vSphere
- Rozwiązanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego oraz fizycznego
- Rozwiązanie musi mieć możliwość wykorzystania wbudowanego kolektora w celach dalszej analizy ruchu
- Rozwiązanie musi mieć możliwość posiadać automatyczne rekomendacje reguł firewall'a na bazie zebranych informacji o przepływach
- Rozwiązanie musi mieć możliwość wizualizacji ścieżki logicznej i przejść w relacji vm-vm, wskazanie komponentów sieciowych w topologii logicznej i fizycznej - przełączników, router'ów, firewall'i oraz połączeń między nimi z uwzględnieniem komponentów wirtualnych
- Rozwiązanie musi mieć możliwość wizualizacji przepływów pomiędzy maszynami wirtualnymi i/lub środowiskiem fizycznym pogrupowanych ze względu na sieci wirtualne, podsieci, aplikacje, grupy bezpieczeństwa

- Rozwiązanie musi mieć możliwość informowania o tym, jakie reguły firewall'a wirtualnego są aktualnie zaaplikowane i aktywne
- Rozwiązanie musi mieć możliwość informowania o maskowanych regułach firewall'a, czyli regułach, które nie są wykorzystywane ze względu na reguły położone wyżej
- Rozwiązanie musi mieć możliwość informowania i wizualizacji połączeń maszyn wirtualnych do zasobów dyskowych, połączenia do hosta i wyjścia na zewnątrz do sieci fizycznej
- Rozwiązanie do analizy przepływów sieciowych musi posiadać funkcjonalność API

Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Zamawiający wymaga, aby w przypadku wystąpienia problemów, wysyłanie zgłoszeń serwisowych do Producenta było zapewnione z poziomu portalu użytkownika, służącego do zarządzania kluczami licencyjnymi do posiadanego oprogramowania do wirtualizacji.

Poziomy zgłoszeń L1, L2, L3,
L1 - przyjęcie zgłoszenia i wyszukanie w bazie wiedzy" czy problem jest powtarzalny i czy nie został już zgłoszony w przeszłości przez któregoś z użytkowników, jeżeli tak jest do użytkownika wysyłana jest informacja z rozwiązaniem problemu,
L2 - dalsza analiza problemu i próba jego odtworzenia. Jeżeli w wyniku analizy okaże się, że problem występuje na poziomie kodu źródłowego oprogramowania, wówczas trafia on na poziom L3,
L3 - opracowywanie poprawek na poziomie kodu źródłowego: patch'y, update'ów, bug-fix'ów, itp.

5. Warunki równoważności dla oprogramowania VMware Site Recovery Manager w wersji Enterprise

- Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych niezależnie od architektury DataCenter (Active-Active, Active-Pasive)
- Rozwiązanie musi posiadać taką architekturę, aby umożliwiać wykonanie planu awaryjnego nawet w przypadku całkowitej niedostępności pojedynczego centrum danych
- Rozwiązanie musi umożliwiać przełączanie maszyn wirtualnych z systemami operacyjnymi minimum: Windows NT, Windows Server 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows XP, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, SLES 8, REH L 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, REHL Atomie 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, 05/2 Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin
- 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
- Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych z dyskami wirtualnymi oraz dyskami udostępnionymi maszynom wirtualnym wprost z macierzy typu Raw Device
- Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych zlokalizowanych na macierzach typu FC, iSCSI, NFS
- Rozwiązanie musi być niezależne od producenta zastosowanego sprzętu fizycznego
- Rozwiązanie musi umożliwiać wykonywanie procedur przełączanie usług IT z ośrodka podstawowego do ośrodka zapasowego (fail-over) i z powrotem (fail-back) w ramach jednego narzędzia/konsoli

- 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
- 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
- Proces przełączania usług IT pomiędzy Centrami Przetwarzania Danych musi być automatyczny tzn. nie wymagający interwencji administratora w żadnej warstwie infrastruktury - CPU, RAM, LAN, SAN
- Rozwiązanie musi umożliwiać tworzenie planów przełączeniowych, konfigurowanie tych planów i przypisywanie do nich maszyn wirtualnych
- Plan przełączeniowy musi umożliwiać:
    a. Tworzenie więcej niż jednego planu przełączeniowego,
    b. Przypisanie jednej lub wielu wirtualnych maszyn,
    c. Określanie kolejności uruchamiania maszyn wirtualnych w momencie przełączenia,
    d. Zatrzymanie wybranych wirtualnych maszyn pracujących w ośrodku zapasowym zwalniając tym samym moc obliczeniową dla przełączanych maszyn,
    e. Zmianę adresacji IP maszyn wirtualnych,
    f. Uruchamianie skryptów konfiguracyjnych w dowolnym momencie procesu przełączenia (w tym w maszynach wirtualnych).
- Rozwiązanie musi umożliwiać ochronę maszyn wirtualnych pracujących w Centrach Przetwarzania o następującej architekturze:
    a. Jeden do Jednego,
    b. Wiele do Jednego,
    c. A do B do C do A.
- Rozwiązanie musi umożliwiać automatyczne generowanie raportów z historycznych przełączeń oraz ich eksportowanie do pliku HTML, XML, CSV, MS Excel lub MS Word
- Ochrona do 75 maszyn wirtualnych
- Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych niezależnie od architektury DataCenter (Active-Active, Active-Pasive, Stretched Cluster)
- Rozwiązanie musi umożliwiać ochronę maszyn wirtualnych z wykorzystaniem funkcjonalności migracji „online" maszyn wirtualnych pomiędzy różnymi konsolami do zarządzania środowiskami wirtualnymi
- Rozwiązanie musi umożliwiać ochronę wirtualnych maszyn w oparciu o technologię macierzową VASA
- Rozwiązanie musi umożliwiać ochronę maszyn wirtualnych poprzez integrację z rozwiązaniem do wirtualizacji sieci (SON).

Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Zamawiający wymaga, aby w przypadku wystąpienia problemów, wysyłanie zgłoszeń serwisowych do Producenta było zapewnione z poziomu portalu użytkownika, służącego do zarządzania kluczami licencyjnymi do posiadanego oprogramowania do wirtualizacji.

Poziomy zgłoszeń L1, L2, L3,
L1 - przyjęcie zgłoszenia i wyszukanie w "bazie wiedzy" czy problem jest powtarzalny i czy nie został już zgłoszony w przeszłości przez któregoś z użytkowników, jeżeli tak jest do użytkownika wysyłana jest informacja z rozwiązaniem problemu,
L2 - dalsza analiza problemu i próba jego odtworzenia. Jeżeli w wyniku analizy okaże się, że problem występuje na poziomie kodu źródłowego oprogramowania, wówczas trafia on na poziom L3,
L3 - opracowywanie poprawek na poziomie kodu źródłowego: patch'y, update'ów, bug-fix'ów, itp.

Załącznik nr 2 - Formularz odpowiedzi na zapytanie

Dane podmiotu	
Adres Wykonawcy: kod, miejscowość, ulica, nr lokalu	
Nr telefonu	
E-mail	

Zakład Ubezpieczeń Społecznych

ul. Szamocka 3, 5

01-748 Warszawa

FORMULARZ ODPOWIEDZI NA ZAPYTANIE O INFORMACJĘ

1. W odpowiedzi na Zapytanie o informację dotyczące ***Zakup licencji VMware do wirtualizacji zasobów serwerowych albo oprogramowania równoważnego*** przedstawiam poniższe informacje.
2. Poniższe informacje (**wybrać właściwe**):
   - *zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i nie mogą być ujawniane innym podmiotom.
   - *nie zawierają informacji stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i mogą być ujawniane innym podmiotom.

   UWAGA: w przypadku gdy Wykonawca nie zaznaczy żadnej z ww. opcji, ZUS przyjmie, że Wykonawca nie zastrzega przekazanych informacji jako stanowiących tajemnicę przedsiębiorstwa, co w konsekwencji oznaczać będzie, że takie informacje będą udostępnianie przez ZUS w trybie dostępu do informacji publicznej, na stosowny wniosek innych podmiotów.

3. Przedstawione informacje dotyczące szacunkowych kosztów (**wybrać właściwe*):
   - *zawierają upusty na poziome ….% od „cen katalogowych".
   - *nie zawierają upustów od „cen katalogowych" i ZUS może uzyskać upust na poziome ….% od poniżej przedstawionych kosztów.

4. Wszelką korespondencję dotyczącą przedmiotowej odpowiedzi na zapytanie o informację należy kierować na:

Imię i Nazwisko	
Nazwa podmiotu	
Adres	
Nr telefonu	
Nr faksu	
Adres e-mail	

Zakup licencji VMware do wirtualizacji zasobów serwerowych

Formularz cenowy

0	1	2	3	4	5	6	7	8	9
Lp.	**Zakres**	**Zaproponowane oprogramowanie (producent, nazwa, sposób licencjonowania)**	**Jednostka**	**Cena jednostkowa w PLN (bez VAT)**	**Stawka podatku VAT w %**	**Cena jednostkowa w PLN (z VAT)**	**Całkowita Liczba**	**Razem w PLN (bez VAT)** (kol. 4 x kol. 7)	**Razem w PLN (z VAT)** (kol. 5 x kol. 6)
1	**VMware vSphere Standard wraz z 36 miesięcznym wsparciem producenta**	**……..****	**Sztuka**	**……..***	**……..***	**……..***	**80**	**……..***	**……..***
2	**VMware vSphere Enterprise Plus wraz z 36 miesięcznym wsparciem producenta**	**……..****	**Sztuka**	**……..***	**……..***	**……..***	**546**	**……..***	**……..***
3	**VMware vSphere Remote Office Branch Office Advanced wraz z 36 miesięcznym wsparciem producenta**	**……..****	**Sztuka**	**……..***	**……..***	**……..***	**…..***	**……..***	**……..***
4	**VMware vCenter Server w wersji Standard wraz z 36 miesięcznym wsparciem producenta**	**……..****	**Sztuka**	**……..***	**……..***	**……..***	**8**	**……..***	**……..***
5	**VMware NSX Data Center w wersji Enterprise Plus wraz z 36 miesięcznym wsparciem producenta**	**……..****	**Sztuka**	**……..***	**……..***	**……..***	**4**	**……..***	**……..***
6	**VMware SRM w wersji Enterprise wraz z 36 miesięcznym wsparciem producenta**	**……..****	**Sztuka**	**……..***	**……..***	**……..***	**50**	**……..***	**……..***
								Razem	**……..***

* wypełnia Oferent

** wypełnia Oferent w przypadku zaproponowania rozwiązania równoważnego