**Załącznik nr 3 do SIWZ**

**OPIS PARAMETRÓW RÓWNOWAŻNYCH**

**(wymagania niezbędne przy zaoferowaniu produktu innego niż wymieniony w punkcie 5.2 SIWZ)**

**Oferowany produkt (nazwa, wersja)……………………………………………………………….**

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

|  |  |
| --- | --- |
| **Minimalne funkcje, parametry techniczne i warunki wymagane** | **Parametry i warunki zaoferowane przez Wykonawcę** |
|  | Możliwość wykorzystania nielimitowanej liczby rdzeni logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym |  |
|  | Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny. |  |
|  | Możliwość budowania klastrów składających się z 64 węzłów. |  |
|  | Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. |  |
|  | Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |  |
|  | Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. |  |
|  | 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). |  |
|  | Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |  |
|  | Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET |  |
|  | Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. |  |
|  | Możliwość wykorzystania standardu http/2. |  |
|  | Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. |  |
|  | Dostępne dwa rodzaje graficznego interfejsu użytkownika: klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy oraz dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. |  |
|  | Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, |  |
|  | Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. |  |
|  | Mechanizmy logowania w oparciu o:* 1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
 |  |
|  | 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. |  |
|  | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |  |
|  | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |  |
|  | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |  |
|  | Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). |  |
|  | Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. |  |
|  | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: |  |
| * 1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
		1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
		4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1, Windows 10.
 |  |
| * 1. Zdalna dystrybucja oprogramowania na stacje robocze.
 |  |
| * 1. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
 |  |
| * 1. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		1. Dystrybucję certyfikatów poprzez http
		2. Konsolidację CA dla wielu lasów domeny,
		3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 |  |
| * 1. Szyfrowanie plików i folderów.
 |  |
| * 1. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
 |  |
| * 1. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
 |  |
| * 1. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 |  |
| * 1. Serwis udostępniania stron WWW.
 |  |
| * 1. Wsparcie dla protokołu IP w wersji 6 (IPv6),
 |  |
| * 1. Wsparcie dla algorytmów Suite B (RFC 4869),
 |  |
| * 1. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 |  |
| * 1. Wbudowane mechanizmy wirtualizacji (hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
 |  |
| * 1. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
 |  |
| * 1. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
 |  |
| * 1. Mechanizmy wirtualizacji mające wsparcie dla:
		1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
		3. Obsługi 4-KB sektorów dysków
		4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
		5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
		6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
		7. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
 |  |
|  | Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów. |  |
|  | Wsparcie dla rozwiązania Kubernetes. |  |
|  | 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. |  |
|  | Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). |  |
|  | Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. |  |
|  | Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |  |
|  | Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |  |
|  | Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |  |
|  | Mechanizm konfiguracji połączenia VPN do platformy Azure. |  |
|  | Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. |  |
|  | Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów. |  |