

Opis Przedmiotu Zamówienia

Dostawa oprogramowania standardowego z licencjami wieczystymi

Spis treści

1. Opis ogólny przedmiotu zamówienia.....	2
1.1. Serwerowy system operacyjny z prawem do aktualizacji do najnowszej wersji w ciągu 36 msc. (licencja na dwa rdzenie procesora)	2
1.2. Serwerowy system operacyjny z prawem do aktualizacji do najnowszej wersji w ciągu 36 msc. typ II (licencja na dwa rdzenie procesora)	6

1. Opis ogólny przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa oprogramowania standardowego z licencjami wieczystymi (Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).

Zamawiający wymaga dostawy Produktów na warunkach przewidzianych przez producenta oprogramowania (Producenta) dla jednostek realizujących zadania publiczne.

Specyfikacja ilościowa przedmiotu zamówienia:

	Typ oprogramowania	liczba Produktów
1	Serwerowy system operacyjny z prawem do aktualizacji do najnowszej wersji w ciągu 36 msc. (licencja na dwa rdzenie procesora)	8
2	Serwerowy system operacyjny z prawem do aktualizacji do najnowszej wersji w ciągu 36 msc. typ II (licencja na dwa rdzenie procesora)	66

Tabela 1 – specyfikacja ilościowa zamawianych produktów.

1.1. Serwerowy system operacyjny z prawem do aktualizacji do najnowszej wersji w ciągu 36 msc. (licencja na dwa rdzenie procesora)

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12. Możliwość wykorzystania standardu http/2.
13. Wbudowana zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - b. Dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych.
15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17. Mechanizmy logowania w oparciu o:
 - a. Login i hasło,
 - b. Karty z certyfikatami (smartcard),
 - c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
18. 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.
19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
22. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
23. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
24. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

- b. 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:
 - i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
- c. Zdalna dystrybucja oprogramowania na stacje robocze.
- d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
- e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http
 - ii. Konsolidację CA dla wielu lasów domeny,
 - iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- f. Szyfrowanie plików i folderów.
- g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- h. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
- i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- j. Serwis udostępniania stron WWW.
- k. Wsparcie dla protokołu IP w wersji 6 (IPv6),
- l. Wsparcie dla algorytmów Suite B (RFC 4869),
- m. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- n. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
- o. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

- p. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- q. Mechanizmy wirtualizacji mające wsparcie dla:
 - i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - iii. Obsługi 4-KB sektorów dysków
 - iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
 - vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
- 25. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
- 26. Wsparcie dla rozwiązania Kubernetes.
- 27. 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.
- 28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- 29. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
- 30. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- 31. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- 32. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- 33. Mechanizm konfiguracji połączenia VPN do platformy Azure.
- 34. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
- 35. Mechanizmy pozwalające na blokadę dostępu nieznanym procesom do chronionych katalogów.
- 36. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

1.2. Serwerowy system operacyjny z prawem do aktualizacji do najnowszej wersji w ciągu 36 msc. typ II (licencja na dwa rdzenie procesora)

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12. Możliwość wykorzystania standardu http/2.
13. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

- b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
 16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
 17. Mechanizmy logowania w oparciu o:
 - a. Login i hasło,
 - b. Karty z certyfikatami (smartcard),
 - c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
 18. 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.
 19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 21. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
 22. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
 23. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
 24. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - r. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - s. 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:
 - i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

- t. Zdalna dystrybucja oprogramowania na stacje robocze.
- u. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
- v. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http
 - ii. Konsolidację CA dla wielu lasów domeny,
 - iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- w. Szyfrowanie plików i folderów.
- x. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- y. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
- z. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- aa. Serwis udostępniania stron WWW.
- bb. Wsparcie dla protokołu IP w wersji 6 (IPv6),
- cc. Wsparcie dla algorytmów Suite B (RFC 4869),
- dd. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- ee. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
- ff. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- gg. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- hh. Mechanizmy wirtualizacji mające wsparcie dla:
 - i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - iii. Obsługi 4-KB sektorów dysków
 - iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

- v. Możliwość wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - vi. Możliwość kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
 - vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
25. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
26. Wsparcie dla rozwiązania Kubernetes.
27. 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.
28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
30. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
31. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
32. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
33. Mechanizm konfiguracji połączenia VPN do platformy Azure.
34. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
35. Mechanizmy pozwalające na blokadę dostępu nieznanym procesom do chronionych katalogów.
36. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.