

Załącznik 4 do OPZ

Wymagania na Serwerowy system operacyjny

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa do siedziby Zamawiającego licencji Serwerowego systemu operacyjnego przeznaczonego dla serwera aplikacyjnego opisanego w Załączniku 2 do OPZ, spełniającej minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich instalacja i konfiguracja.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

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. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 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:
 - 9.1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - 9.2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - 9.3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - 9.4. 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 uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - 15.1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - 15.2. Dotykowy umożliwiający sterowanie dotykkiem 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, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

Zamówienie współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020 w ramach Działania VII.1.2 Technologie informacyjno-komunikacyjne.

18. Mechanizmy logowania w oparciu o:
 - 18.1. Login i hasło,
 - 18.2. Karty z certyfikatami (smartcard),
 - 18.3. 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 większości 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:
 - 25.1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - 25.2. 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:
 - 25.2.1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - 25.2.2. Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - 25.2.3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - 25.2.4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
 - 25.3. Zdalna dystrybucja oprogramowania na stacje robocze.
 - 25.4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
 - 25.5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
 - 25.5.1. Dystrybucję certyfikatów poprzez http
 - 25.5.2. Konsolidację CA dla wielu lasów domeny,
 - 25.5.3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - 25.5.4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 - 25.6. Szyfrowanie plików i folderów.
 - 25.7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
 - 25.8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - 25.9. Serwis udostępniania stron WWW.
 - 25.10. Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - 25.11. Wsparcie dla algorytmów Suite B (RFC 4869),
 - 25.12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 - 25.13. 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:

Zamówienie współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020 w ramach Działania VII.1.2 Technologie informacyjno-komunikacyjne.

- 25.13.1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- 25.13.2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- 25.13.3. Obsługi 4-KB sektorów dysków
- 25.13.4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
- 25.13.5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
- 25.13.6. 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. Licencja musi uprawniać do funkcjonowania na co najmniej 100 corach umożliwiającą uruchomienie na 3 serwerach terminalowych i jednym serwerze backupowym.

Wymagania w zakresie instalacji i konfiguracji:

1. Instalacja i konfiguracja systemu na serwerze
2. Założenie kont administratorów
3. Konfiguracja definicji zasad grup według wskazówek Zamawiającego.
4. Konfiguracja usług do pracy w istniejącym środowisku sieciowym.
5. Podłączenie do domeny wskazanej przez Zamawiającego
6. Stworzenie udostępnionych udziałów sieciowych według wskazówek zamawiającego.
7. Konfiguracja usług ról przestrzeni nazw systemu plików DFS i replikacji systemu plików DFS, które składają się na rozproszony system plików według wskazówek Zamawiającego