|  |  |
| --- | --- |
| **TABELA A1  W przypadku oferowania produktu równoważnego w stosunku do Tabela A- serwer rack, pozycja „System operacyjny”:** | |
|  | W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022/2025 , Zamawiający wymaga dostarczenia odpowiedniej ilości licencji dla serwera fizycznego oraz serwerów wirtualnych, oraz instalację i migrację obecnego środowiska. Zamawiający wymaga aby produkt równoważny spełniał niżej wymienione wymagania:   1. Współpraca z procesorami o architekturze x86 – 64bit. 2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. 3. Możliwość budowania klastrów składających się z 64 węzłów. 4. Licencja/licencje muszą obsłużyć serwer fizyczny wyposażony w zaproponowane procesory / fizyczne rdzenie. 5. Praca w roli klienta domeny Microsoft Active Directory. 6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2019. 7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. 8. Możliwość uruchomienia roli klienta i serwera czasu (NTP). 9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 11. Możliwość uruchomienia roli serwera stron WWW. 12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. 13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego. 14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). 15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:     1. pozwalają na zmianę rozmiaru w czasie pracy systemu,     2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,     3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,     4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość 19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 22. Możliwość wykorzystania standardu http/2. 23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 26. Mechanizmy logowania w oparciu o: a) login i hasło,     1. karty z certyfikatami (smartcard),     2. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:     1. określonych grup użytkowników,     2. zastosowanej klasyfikacji danych,     3. centralnych polityk dostępu w sieci,     4. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 33. 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:        * + podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,          + ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,          + 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.,     3. zdalna dystrybucja oprogramowania na stacje robocze,     4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,     5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        * + Dystrybucję certyfikatów poprzez http,          + Konsolidację CA dla wielu lasów domeny,          + Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,          + Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     6. szyfrowanie plików i folderów,     7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),     8. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,     9. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,     10. serwis udostępniania stron WWW,     11. wsparcie dla protokołu IP w wersji 6 (IPv6),     12. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,     13. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),     14. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.     15. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.     16. mechanizmy wirtualizacji mające wsparcie dla:         * + dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,           + obsługi ramek typu jumbo frames dla maszyn wirtualnych.           + obsługi 4-KB sektorów dysków,           + nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,           + możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.     17. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.     18. wsparcie dla rozwiązania Kubernetes.     19. 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.     20. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).     21. mechanizmy deduplikacji i kompresji na wolumenach.     22. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.     23. mechanizm konfiguracji połączenia VPN do platformy Azure.     24. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.     25. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.     26. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL )Server Standard). |
| Zapewniający pełną kompatybilność z istniejąca infrastrukturą Zamawiającego, a w szczególności z posiadanym oprogramowaniem  -praca jako stacje końcowe PC | w pełni kompatybilny z posiadanym oprogramowaniem Zamawiającego, pozwalający uruchamiać poniższe oprogramowanie bezpośrednio z poziomu systemu operacyjnego, bez dodatkowego oprogramowania (emulatora) lub warstwy wirtualizacyjnej :  **Do każdego poniższego oprogramowania wymagane oświadczenie producenta** oprogramowania o zgodności z proponowanym systemem operacyjnym (oświadczenie należy dostarczyć Zamawiającemu wraz ze sprzętem komputerowym).   1. system finansowo-księgowy ZSI SIGID (https://sigid.pl/) 2. system sprawozdawczości Besti@ (<https://budzetjst.pl/>) 3. Rejestr Zaangażowania Środków Budżetowych-Doskomp (https://portal.jst.pl/) 4. Legislator (<https://www.abcpro.pl/eap-legislator>) 5. Axence nVision 6. Eset XDR |