# Opis przedmiotu zamówienia
# **CZĘŚĆ II** - Serwery
# Minimalne wymagania techniczne dla:

## A. Serwera kasetowego typu „Blade" 192Gb z systemem operacyjnym **do montażu** w obudowie kasetowej DELL M1000 – szt. 4

Obudowa - Typu blade, umożliwiająca zainstalowanie min. 16 sztuk serwerów (typu jak zaoferowany) w posiadanej przez Zamawiającego obudowie DELL Blade M1000e.

**Płyta główna** - Płyta główna z możliwością zainstalowania do dwóch procesorów cztero, sześcio ośmio, dziesięcio, dwunasto, czternasto, szesnasto, osiemnasto, dwudziesto- rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

Chipset - Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Procesor - Dwa procesory ośmio-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 667 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera.

**Pamięć RAM** - 192GB pamięci RAM typu RDIMM o częstotliwości pracy min. 2400MT/s Płyta powinna obsługiwać do 1.5TB pamięci RAM, na płycie głównej powinno znajdować się minimum 12 slotów wolnych przeznaczonych na rozbudowę. Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep.

Karta graficzna - Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024

Wbudowane porty - min. 3x USB 2.0 z czego 2 na przednim panelu obudowy obsługujące bootowanie z napędów: dyskietek, CD/DVD, klucza USB. Zamawiający nie dopuszcza realizacji poprzez zastosowanie przejściówek, adapterów oraz modułów lub kabli rozszerzających.

Interfejsy LAN - Min. 2 interfejsy 10GbE konwergentne. Karta powinny obsługiwać funkcjonalność dzielenia każdego z interfejsów na minimum 2 wirtualne partycje z własnym MAC adresem. Rozwiązanie to musi być niezależne od zainstalowanego na serwerze systemu operacyjnego.

Interfesy SAN - Min. 2 interfejsy FC8 Gb/s

**Wewnętrzna pamięć masowa** - Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS, SSD oraz zamoszyfrujących dostępnych w aktualnej ofercie producenta serwera. Zainstalowane 2 dyski twarde o pojemności min. 300GB SAS 12Gb/s 15k fabrycznie skonfigurowane w RAID 1. Możliwość instalacji wewnętrznych modułów dedykowanych dla hypervisora wirtualizacyjnego, wyposażonego w dwa jednakowe nośniki typu flash o pojemności min. 16GB z możliwością skonfigurowania zabezpieczenia typu "mirror" pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

**Bezpieczeństwo** - Zintegrowany z płytą główną moduł TPM.

Karta za**rządzająca** - Niezależna od zainstalowanego na serwerze systemu operacyjnego umożliwiająca:
- zdalny dostęp do graficznego interfejsu Web karty zarządzającej,

- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera),
- szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika,
- możliwość podmontowania zdalnych wirtualnych napędów,
- wirtualną konsolę z dostępem do myszy, klawiatury,
- wsparcie dla IPv6,
- wsparcie dla: SNMP; IPMI2.0, VLAN tagging, Telnet, SSH,
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer,
- integracja z Active Directory,
- możliwość obsługi przez dwóch administratorów jednocześnie,
- wsparcie dla dynamic DNS,
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,
- automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) zapisanych na dedykowanej pamięci flash wbudowanej na karcie zarządzającej.

Gwarancja – Min. 36 m-cy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Firma serwisująca musi posiadać ISO 9001: 2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera

Certyfikaty - Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2008 R2 x64, Windows Server 2012 R2, Windows Server 2016.

Dokumentacja - Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

System operacyjny - Microsoft Windows Server 2016 Datacenter lub równoważny, spełniający wymienione poniżej minimalne wymagania:
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:
    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).
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 uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    1) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    2) Dotykowy umożliwiający sterowanie dotykiem 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.
18. 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),
19. Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników.
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:
    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:

a) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
b) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
c) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
d) 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,
5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   a) Dystrybucję certyfikatów poprzez http,
   b) Konsolidację CA dla wielu lasów domeny,
   c) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   d) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
1) Szyfrowanie plików i folderów,
2) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
3) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
4) Serwis udostępniania stron WWW,
5) Wsparcie dla protokołu IP w wersji 6 (IPv6),
6) Wsparcie dla algorytmów Suite B (RFC 4869),
7) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. 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:
   a) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   b) Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
   c) Obsługi 4-KB sektorów dysków,
   d) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
   e) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
   f) 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 Strona 6 z 12 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. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim (w przypadku zaoferowania rozwiązania równoważnego).

## B. Serwera kasetowego typu „Blade" 64 Gb z systemem **operacyjnym do montażu** w obudowie kasetowej DELL M1000 – szt. 1

Obudowa - Typu blade, umożliwiająca zainstalowanie min. 16 sztuk serwerów (typu jak zaoferowany) w posiadanej przez zamawiajacego obudowy DELL Blade M1000e.

**Płyta główna** - Płyta główna z możliwością zainstalowania do dwóch procesorów cztero, sześcio ośmio, dziesięcio, dwunasto, czternasto, szesnasto, osiemnasto, dwudziesto- rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

Chipset - Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Procesor - Dwa procesory ośmio-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 667 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera.

**Pamięć RAM** – 64 GB pamięci RAM typu RDIMM o czestotliwości pracy min. 2400MT/s Płyta powinna obsługiwać do 1.5TB pamięci RAM, na płycie głównej powinno znajdować się minimum 12 slotów wolnych przeznaczonych na rozbudowę. Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep.

Karta graficzna - Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024

Wbudowane porty - min. 3x USB 2.0 z czego 2 na przednim panelu obudowy obsługujące bootowanie z napędów: dyskietek, CD/DVD, klucza USB. Zamawiający nie dopuszcza realizacji poprzez zastosowanie przejściówek, adapterów oraz modułów lub kabli rozszerzających.

Interfejsy LAN - Min. 2 interfejsy 10GbE konwergentne. Karta powinny obsługiwać funkcjonalność dzielenia każdego z interfejsów na minimum 2 wirtualne partycje z własnym MAC adresem. Rozwiązanie to musi być niezależne od zainstalowanego na serwerze systemu operacyjnego.

Interfesy SAN - Min. 2 interfejsy FC8 Gb/s

**Wewnętrzna pamięć masowa** - Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS, SSD oraz zamoszyfrujących dostępnych w aktualnej ofercie producenta serwera. Zainstalowane 2 dyski twarde o pojemności min. 300GB SAS 12Gb/s 15k fabrycznie skonfigurowane w RAID 1. Możliwość instalacji wewnętrznych modułów dedykowanych dla hypervisora wirtualizacyjnego, wyposażonego w dwa jednakowe nośniki typu flash o pojemności min. 16GB z możliwością skonfigurowania zabezpieczenia typu "mirror" pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

**Bezpieczeństwo** - Zintegrowany z płytą główną moduł TPM.

Karta za**rządzająca** - Niezależna od zainstalowanego na serwerze systemu operacyjnego umożliwiająca:
- zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera),
- szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika,

- możliwość podmontowania zdalnych wirtualnych napędów,
- wirtualną konsolę z dostępem do myszy, klawiatury,
- wsparcie dla IPv6,
- wsparcie dla: SNMP; IPMI2.0, VLAN tagging, Telnet, SSH,
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer,
- integracja z Active Directory,
- możliwość obsługi przez dwóch administratorów jednocześnie,
- wsparcie dla dynamic DNS,
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,
- automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) zapisanych na dedykowanej pamięci flash wbudowanej na karcie zarządzającej.

Gwarancja – Min. 36 m-cy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Firma serwisująca musi posiadać ISO 9001: 2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera.

Certyfikaty - Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2008 R2 x64, Windows Server 2012 R2, Windows Server 2016.

Dokumentacja - Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

System operacyjny - Microsoft Windows Server 2016 Standard lub równoważny, spełniający wymienione poniżej wymagania:
Licencje na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.
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:
    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).
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 uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    1) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    2) Dotykowy umożliwiający sterowanie dotykiem 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.
18. 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),
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:
    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:

a) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
b) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
c) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
d) 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,
5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   a) Dystrybucję certyfikatów poprzez http,
   b) Konsolidację CA dla wielu lasów domeny,
   c) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   d) 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) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
9) Serwis udostępniania stron WWW,
10) Wsparcie dla protokołu IP w wersji 6 (IPv6),
11) Wsparcie dla algorytmów Suite B (RFC 4869),
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 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:
   a) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   b) Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
   c) Obsługi 4-KB sektorów dysków,
   d) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
   e) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
   f) 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. Nośnik i klucz produktu pochodzący od producenta sprzętu,
32. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim (w przypadku zaoferowania rozwiązania równoważnego).