

1. Serwer – ilość 2 szt. oraz 3 licencje na Serwerowy system operacyjny

LP	Parametr lub warunek	Minimalne wymagania
1	Obudowa	-Typu Rack, wysokość maksimum 1U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack; -Możliwość montażu ramki na froncie obudowy serwera zabezpieczającej dyski przed nieuprawnionym wysunięciem;
2	Płyta główna	-Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; -wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem -Minimum 4 złącza PCI Express generacji 4, w tym minimum 3 złącza o prędkości x16; -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; -Zainstalowany moduł TPM 2.0 (współpracujący z Windows Serwer 2022)
3	Procesory	Zainstalowany jeden procesor 16-rdzeniowy w architekturze x86, osiągający wynik w testach wydajności SPECrate2017_int_base min. 222 pkt. przy konfiguracji z dwoma procesorami dla dowolnej platformy dwuprocesorowej producenta serwera, który jest oferowany w postępowaniu przez oferenta. Wymagamy aby był załączony PDF ze strony spec.org; Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych;
4	Pamięć RAM	-Zainstalowane 128 GB pamięci RAM typu DDR4 Registered, 3200Mhz w kościach o pojemności 32GB; -Wsparcie dla technologii zabezpieczania pamięci ECC, Memory Scrubbing, SDDC lub równoważnej; -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM (memory mirror);
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60, 2GB pamięci podręcznej cache oraz utrzymaniem pamięci podręcznej;
6	Dyski twarde	-Zainstalowane 2 dyski SSD, minimum 480GB każdy, o parametrze DWPD minimum 1, dyski hotplug; -Minimum 8 wnęk dla dysków Hotplug 2,5 cala;
8	Kontrolery LAN	-Karta sieciowa LAN, 2x10Gbit/s SFP+, niezajmująca slotu PCI Express (dopuszcza się instalację w slotcie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilość slotów PCI Express), dostarczona wraz z wkładami 10GB MultiMode; -Możliwość instalacji dodatkowej karty sieciowej niezajmującej slotu PCI Express;
9	Kontrolery I/O FC/SAS/Inne	-Zainstalowana karta 2x FC 16GB;
10	Porty	-zintegrowana karta graficzna ze złączem VGA z tyłu serwera; -2x USB 3.0 dostępne na froncie obudowy -2x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;
11	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o mocy maksymalnej min. 500W każdy, o sprawności 94% (tzw klasa Platinum); -Redundantne wentylatory hotplug; -Serwer dostarczony wraz z dwoma kablami C13-C14 o długości min. 2,5m każdy;
12	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zarządzającej serwerem, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. Wymaga się aby system rozpoznawania awarii był niezależny od zasilania i działał (wskazywał uszkodzony element) po odłączeniu kabli zasilających serwera (podtrzymywany kondensatorowo lub baterijnie w celu uruchomienia przy odłączonym zasilaniu sieciowym).

		<p>-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p> <ul style="list-style-type: none"> • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejścia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) • Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera, umożliwiającego konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
13	System operacyjny	Serwer ma być dostarczony wraz z systemem operacyjnym opisanym w pkt „Serwerowy system operacyjny” oraz umożliwić uruchomienie 6 maszyn wirtualnych;
14	Gwarancja	<p>-3 lata gwarancji producenta serwera w trybie onsite z czasem reakcji w miejscu instalacji serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki;</p> <p>-Dostępność części zamiennych co najmniej przez 3 lat od momentu zakupu serwera;</p> <p>-Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;</p>
15	Dokumentacja, inne	<p>-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie.</p> <p>-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej. Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;</p> <p>-Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, <u>w ofercie należy podać nr telefonu</u>) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;</p> <p>-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;</p> <p>-Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia. Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania.</p>

Serwerowy system operacyjny

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

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:
 - 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).
- 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:
 - a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - b) 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:
 - a) Login i hasło,
 - b) Karty z certyfikatami (smartcard),
 - c) 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:
- 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
 - 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) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - i) Serwis udostępniania stron WWW.
 - j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - k) Wsparcie dla algorytmów Suite B (RFC 4869),
 - l) 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:
 - 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)

- 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) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim
- 32) Serwerowy system operacyjny w najnowszej wersji producenta oprogramowania dostępnej na rynku.

2. Serwer backup – ilość 1 szt.

LP	Parametr lub warunek	Minimalne wymagania
1	Obudowa	-Typu Rack, wysokość maksimum 1U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack; -Możliwość montażu ramki na froncie obudowy serwera zabezpieczającej dyski przed nieuprawnionym wysunięciem;
2	Płyta główna	-Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; -wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem -Minimum 4 złącza PCI Express generacji 4, w tym minimum 3 złącza o prędkości x16; -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; -Zainstalowany moduł TPM 2.0 (współpracujący z Windows Serwer 2022)
3	Procesory	Zainstalowany jeden procesor 16-rdzeniowy w architekturze x86, osiągający wynik w testach wydajności SPECrate2017_int_base min. 222 pkt. przy konfiguracji z dwoma procesorami dla dowolnej platformy dwuprocesorowej producenta serwera, który jest oferowany w postępowaniu przez oferenta. Wymagamy aby był załączony PDF ze strony spec.org; Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych;
4	Pamięć RAM	-Zainstalowane 128 GB pamięci RAM typu DDR4 Registered, 3200Mhz w kościach o pojemności 32GB; -Wsparcie dla technologii zabezpieczania pamięci ECC, Memory Scrubbing, SDDC lub równoważnej; -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM (memory mirror);
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60, 2GB pamięci podręcznej cache oraz utrzymaniem pamięci podręcznej;
6	Dyski twarde	-Zainstalowane 4 dyski SAS 12G, minimum 4TB każdy, o prędkości obrotowej 7,2k, dyski hotplug; -Minimum 4 wnęk dla dysków Hotplug 3,5 cala;
8	Kontrolery LAN	-Karta sieciowa LAN, 2x10Gbit/s SFP+, niezajmująca slotu PCI Express (dopuszcza się instalację w slotcie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilość slotów PCI Express), dostarczona wraz z wkładami 10GB MultiMode; -Możliwość instalacji dodatkowej karty sieciowej niezajmującej slotu PCI Express;
10	Porty	-zintegrowana karta graficzna ze złączem VGA z tyłu serwera; -2x USB 3.0 dostępne na froncie obudowy -2x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;

11	Zasilanie, chłodzenie	<p>-Redundantne zasilacze hotplug o mocy maksymalnej min. 500W każdy, o sprawności 94% (tzw. klasa Platinum);</p> <p>-Redundantne wentylatory hotplug;</p> <p>-Serwer dostarczony wraz z dwoma kablami C13-C14 o długości min. 2,5m każdy;</p>
12	Zarządzanie	<p>-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zarządzającej serwerem, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. Wymaga się aby system rozpoznawania awarii był niezależny od zasilania i działał (wskazywał uszkodzony element) po odłączeniu kabli zasilających serwera (podtrzymywany kondensatorowo lub baterijnie w celu uruchomienia przy odłączonym zasilaniu sieciowym).</p> <p>-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p> <ul style="list-style-type: none"> • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejścia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Karta zarządzająca musi sprzętowo wspierać virtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - virtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) • Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera, umożliwiającego konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
13	System operacyjny	<p>- Serwer ma być dostarczony wraz z systemem operacyjnym opisanym w pkt „Serwerowy system operacyjny”;</p>
14	Gwarancja	<p>-3 lata gwarancji producenta serwera w trybie onsite z czasem reakcji w miejscu instalacji serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki;</p> <p>-Dostępność części zamiennych co najmniej przez 3 lat od momentu zakupu serwera;</p> <p>-Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;</p>
15	Dokumentacja, inne	<p>-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).</p> <p>-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej. Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;</p> <p>-Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;</p> <p>-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;</p>

		-Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia. Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania.
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Serwerowy system operacyjny

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

- 33) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
- 34) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
- 35) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
- 36) 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.
- 37) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- 38) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- 39) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- 40) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
- 41) 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).
- 42) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 43) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- 44) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
- 45) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

- 46) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 47) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
- a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
- 48) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
- 49) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- 50) 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),
- 51) 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..
- 52) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- 53) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- 54) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 55) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- 56) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- 57) 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. Ustawianie 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
 - e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http
 - ii. Konsolidację CA dla wielu lasów domeny,
 - iii. Automatyczne rejestrowanie 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) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - i) Serwis udostępniania stron WWW.
 - j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - k) Wsparcie dla algorytmów Suite B (RFC 4869),
 - l) 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:
 - 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)
- 58) 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.
- 59) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- 60) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- 61) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- 62) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- 63) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim
- 64) Serwerowy system operacyjny w najnowszej wersji producenta oprogramowania dostępnej na rynku.

3. Macierz dyskowa

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
1.	Obudowa	<p>1) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych, kontrolujących wszystkie zasoby dyskowe macierzy z poziomu pojedynczej konsoli WebGUI/CLI administratora;</p> <p>2) Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez kontrolery i dyski dla zapisów danych Użytkownika;</p> <p>3) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie;</p> <p>4) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia);</p> <p>5) Każdy moduł/obudowa macierzy powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii;</p> <p>6) Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy;</p> <p>7) Moduły dla dalszej rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać gęstości upakowania co najmniej 24 dysków 2,5” lub co najmniej 12 dysków 3,5” na każde 2U przestrzeni instalacyjnej w szafie przemysłowej rack standardu 19”;</p> <p>8) Dostarczona konfiguracja macierzy musi pozwalać na połączenie kaskadowe lub w układzie pętli pomiędzy modułami rozwiązania (moduł kontrolerów, moduły/półki dyskowe), z wykorzystaniem minimum 2-torów kablowych w tych połączeniach – okablowanie to musi być zgodne ze standardem SAS 12Gb/s. W przypadku braku obsługi połączeń w układzie pętli dopuszcza się jako alternatywne rozwiązanie macierz z zainstalowanymi 4 kontrolerami RAID;</p>
2.	Pojemność	<p>1) Oferowana macierz musi obsługiwać min. 142 dyski wykonane w technologii hot-plug – jeżeli dla obsługi tej funkcjonalności konieczny jest zakup dodatkowych licencji to należy ją dostarczyć wraz z macierzą;</p> <p>2) Model oferowanej macierzy musi obsługiwać przestrzeń dyskową w trybie tzw. surowym (RAW) minimum 4000 TB, bez konieczności wymiany zainstalowanych kontrolerów – wymagana zgodność z zapisami aktualnej na moment składania oferty specyfikacji technicznej macierzy, udostępnionej publicznie na stronie internetowej producenta lub jego przedstawiciela w Polsce;</p> <p>3) Model oferowanej macierzy musi umożliwiać rozbudowę do wyższego modelu z tej samej rodziny urządzeń w trybie w „data-in-place” tj. z wykorzystaniem wszystkich modułów półek rozszerzeń dyskowych wykorzystywanych przed rozbudową i z dostępem do wcześniej zapisanych danych;</p> <p>4) Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika;</p>
3.	Kontrolery	<p>1) Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;</p> <p>2) Każdy z kontrolerów macierzy musi posiadać po minimum 16 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;</p> <p>3) Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 1,6 TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD,</p> <p>4) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik;</p> <p>5) Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia – wymaganie w przypadku konfiguracji z min. 2 kontrolerami;</p> <p>6) Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach;</p> <p>7) Każdy z kontrolerów RAID powinien posiadać dedykowane minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy;</p> <p>8) Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej;</p>

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		<p>9) Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC/SAS SAN oraz NAS;</p> <p>10) Dla obsługi operacji blokowych I/O w sieci IP/FC/SAS SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC 32/16Gb/s, iSCSI 10/1Gb/s, SAS 12Gb/s;</p> <p>11) Dla obsługi operacji plikowych I/O w sieci NAS kontrolery macierzy muszą wspierać minimum protokoły dostępu: CIFS, NFS. Obecnie nie jest wymagana obsługa protokołów CIFS, NFS, ale musi istnieć możliwość rozbudowy o tą funkcjonalność. Rozbudowa o tą funkcjonalność nie może wymagać montażu żadnych zewnętrznych elementów/modułów poza obudową macierzy;</p> <p>12) Uruchomienie obsługi protokołów CIFS i NFS nie może powodować zmniejszenia rozmiaru pamięci podręcznej cache wykorzystywanej przez macierz do obsługi protokołów blokowych – jako równoważność dla tego wymagania dopuszczone jest skonfigurowanie dodatkowo minimum po 16GB pamięci podręcznej Cache dla każdego kontrolera lub 2 grup dyskowych RAID1z dyskami SAS SSD minimum 200GB – nie jest wymagane dostarczenie tej funkcjonalności w postępowaniu, możliwość rozbudowy w przyszłości;</p> <p>13) Kontrolery macierzy muszą obsługiwać do 72 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów;</p>
4.	Interfejsy	<p>1) Oferowana macierz musi posiadać minimum:</p> <ul style="list-style-type: none"> - 2 porty FC 16Gb/s (obsadzone wkładkami), przeznaczone do dołączenia serwerów, wyprowadzone na każdy kontroler RAID; <p>2) Macierz musi umożliwiać wymianę portów do transmisji danych(z serwerami) na porty obsługujące protokoły: FC 32Gb/s, iSCSI 1Gb/s, SAS 12Gb/s;</p> <p>3) Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, a w przypadku konieczności licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencją na instalację i obsługę każdego z wymienionych protokołów transmisji danych;</p>
5.	Poziomy RAID	Macierz musi zapewniać poziom zabezpieczenia danych na dyskach, definiowany poziomami RAID: 0, 1, 10, 5, 50, 6;
6.	Wspierane dyski	<p>1) Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex;</p> <p>2) Oferowana macierz musi wspierać dyski hot-plug:</p> <ul style="list-style-type: none"> - dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s i SAS6Gb/s - dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm, <p>3) Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD (SAS i NLSAS) zainstalowanych w dowolnym module rozwiązania;</p> <p>4) Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5" i 3,5";</p> <p>5) Macierz musi obsługiwać min. 72 dyski SAS SSD w całym rozwiązaniu;</p> <p>6) Wymagane jest dostarczenie macierzy zawierającej min. 2 dyski SAS o pojemności min. 1,8 TB każdy, o prędkości obrotowej 1000 obr/min oraz min. 5 dysków SSD o pojemności min 960GB każdy;</p> <p>7) Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach:</p> <ul style="list-style-type: none"> - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID - hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID; <p>8) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess);</p> <p>9) Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych na zainstalowanych dyskach dowolnego typu – funkcjonalność realizowana bezpośrednio przez kontrolery macierzy dla danych blokowych – minimum AES 256. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy.</p>
7.	Opcje software'owe	<p>1) Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 1024 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariantcie dla maksymalnej pojemności dyskowej dla oferowanej macierzy;</p> <p>2) Macierz musi umożliwiać zdefiniowanie min. 4096 woluminów (LUN);</p> <p>3) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączenia macierzy;</p>

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		<p>4) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową;</p> <p>5) Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server 2012R2/2016/2019, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, HP-UX, IBM AIX, SUN Solaris, VMWare , Citrix XEN Server.</p> <p>6) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem);</p> <p>7) Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;</p> <p>8) Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication;</p> <p>9) Replikacja danych jak w pkt.7 musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych;</p> <p>10) Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;</p> <p>11) W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów;</p> <p>12) Macierz musi obsługiwać dla interfejsów iSCSI i interfejsów obsługujących protokoły CIFS i NFS adresacje IP v.4 i IP v.6;</p> <p>13) W przypadku korzystania z protokołów dostępu plikowego obsługa CIFS i NFS musi odbywać się jednocześnie;</p> <p>14) Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy;</p> <p>15) Model oferowanej macierzy musi wspierać rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami ;</p> <p>16) Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;</p> <p>17) Pod użytym w pkt. 15 pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej;</p> <p>18) Dla uruchomienia funkcjonalności ‘klastra macierzowego’ musi być możliwość wykorzystania istniejącej infrastruktury FC/IP SAN Użytkownika w zakresie przełączników FC/Ethernet i kart HBA FC/Ethernet zainstalowanych w serwerach Użytkownika;</p> <p>19) Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie ‘klastra macierzowego’, musi wspierać poziomy RAID1, RAID10, RAID5, RAID6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną;</p> <p>20) Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover);</p> <p>21) Funkcjonalność ‘klastra macierzowego’ musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover);</p> <p>22) Funkcjonalność ‘klastra macierzowego’ musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback);</p> <p>23) Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi</p>

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		<p>technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;</p> <p>24) Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NLSAS;</p> <p>25) Macierz musi pozwalać na definiowanie minimum 32 różnych polityk i zasad migrowania danych w obrębie tej samej macierzy;</p> <p>26) Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB;</p> <p>27) Mechanizm AST musi być wyposażony w funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;</p> <p>28) Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny;</p> <p>29) Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O;</p> <p>30) Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN;</p>
8.	Konfiguracja, zarządzanie	<p>1) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS) jak i do obsługi transmisji protokołami CIFS/NFS;</p> <p>2) Oprogramowanie zarządzające musi być dostarczone w wariantach dla maksymalnej obsługiwanej pojemności dyskowej macierzy oraz dla maksymalnej liczby dysków wspieranej przez oferowaną macierz;</p> <p>3) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.</p> <p>4) Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora;</p> <p>5) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI ;</p>
9.	Gwarancja i serwis	<p>1) Macierz dyskowa musi zostać objęta minimum 36 miesięcznym okresem gwarancji producenta w trybie onsite z czasem reakcji najpóźniej w następnym dniu roboczym od dnia zgłoszenia usterki. Wymagane jest pisemne poświadczenie gotowości realizacji wymaganego poziomu serwisowego przez polskiego przedstawiciela producenta macierzy. Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne.</p> <p>3) Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia, w ciągu 60 miesięcy od daty zakupu;</p> <p>4) Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązanie bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy;</p> <p>5) Macierz musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu o usterce przez samo urządzenie (poprzez dedykowany system wbudowany w macierz - bez pośrednictwa administratora, nie dopuszcza się użycia ogólnodostępnych mechanizmów - poczty email w tym m.in. protokołu SNMP i SMTP, nie dopuszcza się SMS – Zamawiający nie dopuszcza możliwości komunikacji z/do macierzy poprzez pocztę email/SNMP/SMTP itp. z powodów bezpieczeństwa). Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy.</p> <p>6) Macierz musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi</p>

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		<p>reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych;</p> <p>7) Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia;</p> <p>8) Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje;</p>

4. UTM OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

INTRUSION PREVENTION SYSTEM (IPS)

12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
20. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

KSZTAŁTOWANIE PASMA (Traffic Shapping)

21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
 - a. białe/czarne listy,

- b. DNS RBL,
 - c. Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
- a. PPTP VPN,
 - b. IPSec VPN,
 - c. SSL VPN.
35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

40. Urządzenie ma posiadać wbudowany filtr URL.
41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
42. Administrator ma mieć możliwość dodawania własnych kategorii URL.
43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
- a. blokowanie dostępu do adresu URL,
 - b. zezwolenie na dostęp do adresu URL,
 - c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
47. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

49. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
- a. lokalną bazę użytkowników (wewnętrzny LDAP),
 - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
 - c. usługę katalogową Microsoft Active Directory.

- 50. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
- 51. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
 - a. SSL,
 - b. Radius,
 - c. Kerberos.
- 52. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
- 53. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
- 54. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

- 55. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
- 56. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:
 - a. równoważenie względem adresu źródłowego,
 - b. równoważenie względem połączenia.
- 57. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
- 58. Urządzenie ma umożliwiać przełączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).
- 59. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.
- 60. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).
- 61. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

- 62. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
- 63. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.
- 64. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
- 65. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

- 66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
- 67. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
- 68. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
- 69. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

- 70. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH)
- 71. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
- 72. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
- 73. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
- 74. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
- 75. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
 - a. manualnego eksportu do pliku w dowolnym momencie czasu,
 - b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
- 76. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
- 77. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

RAPORTOWANIE

- 78. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- 79. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
- 80. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
- 81. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
- 82. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
- 83. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
- 84. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
- 85. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

- 86. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
- 87. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
- 88. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
- 89. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
- 90. Urządzenie ma posiadać usługę DNS Proxy.
- 91. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

92. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
93. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

94. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
95. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
96. Liczba portów Ethernet 10/100/1000Mbps – min.8.
97. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
98. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
99. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.4Gbps.
100. Przepustowość filtrowania Antywirusowego – minimum 495Mbps.
101. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps.
102. Maksymalna liczba tuneli VPN IPsec – minimum 100.
103. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
104. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
105. Obsługa interfejsów 802.11q (VLAN) – minimum 128
106. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 18 000 nowych sesji/sekundę.
107. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
108. Urządzenie nie ma limitu na liczbę użytkowników.
109. Liczba reguł filtrowania – minimum 8 192.
110. Liczba tras statycznego routingu – minimum 512.
111. Liczba tras dynamicznego routingu – minimum 10 000.

5. Oprogramowanie do tworzenia backupu 6 VM Hyper-V z dwóch serwerów ze wsparciem na 1 rok. – 2 szt.

Wymagania ogólne:

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API

Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastora

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.

Oprogramowanie musi posiadać wsparcie dla NDMP

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAAI, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA

Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: o Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
Rozwiązanie musi wspierać systemy operacyjne macOS
Rozwiązanie musi wspierać wykonywanie kopii zapasowych następujących systemów plików: o NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Btrfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2
Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
Rozwiązanie musi wspierać backup podłączonych dysków USB
Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na: o Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny o Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire o Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS. o Zcentralizowanym repozytorium danych o Bezpośrednio na zasobach Chmury
Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
Rozwiązanie musi wspierać kontrolę pasma sieciowego
Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
Rozwiązanie musi wspierać technologię BitLocker
Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania

Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla: <ul style="list-style-type: none"> o Microsoft Exchange 2010 i nowszych o Microsoft Active Directory 2003 i nowszych o Microsoft Sharepoint 2010 i nowszych o Microsoft SQL 2005 i nowszych o Oracle 11g i nowszych
Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
Rozwiązanie musi wspierać szyfrowanie
Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

6. Zasilacz awaryjny UPS

Moc pozorna 1000 VA

Moc czynna 600 W

Architektura UPS-a line-interactive

Liczba faz na wejściu 1 (230V)

Czas podtrzymania (obciążenie 100%) 9.2 min

Czas ładowania 3 h

Typ obudowy Rack maksymalnie 2 U

Porty zasilania we. IEC-C14

Porty zasilania wy. 4 x IEC-C13

1 x USB (Type B)

1 x RJ-45 (iLO Remote Management Network)

Hałas słyszalny w odległości 1 m od powierzchni urządzenia 42.0dBA

Rozpraszanie ciepła w trybie online 46.0BTU/godz.

Kształt fali wyjściowej Sinusoida

Zabezpieczenie: odcięcie obwodu

W zestawie

CD z oprogramowaniem

CD z dokumentacją

Instrukcja instalacji

Kabel USB

7. Notebook z oprogramowaniem

Procesor klasy x86. Powinien osiągać minimalnie w teście wydajności PassMark PerformanceTest (wynik dostępny na stronie internetowej: https://www.cpubenchmark.net/cpu_list.php) co najmniej wynik 9 980 punktów Passmark CPU Mark (Załączyć do oferty wydruk).

Przekątna ekranu 15,6"
Rozdzielczość 1920 x 1080 (FHD 1080)
Powierzchnia matrycy Matowa
Technologia podświetlania LED
Typ matrycy TFT WVA
Model karty graficznej zintegrowana
Zainstalowana pamięć RAM 8 GB
Maks. wielkość pamięci 32 GB
Liczba obsadzonych gniazd pamięci 1
Liczba wolnych gniazd pamięci 1
Rodzaj pamięci SODIMM DDR4
Pojemność SSD 256 GB
Format szerokości SSD M.2
Interfejs dysku SSD PCI-Express
Komunikacja
LAN 10/100/1000
WiFi 802.11 ac
Bluetooth
1 x USB 2.0 Type-A
1 x USB 3.0 Type-A
Porty wideo 1 x HDMI
Czytnik kart pamięci
1 x Audio (Combo)
1 x RJ-45
Kamera internetowa
Podświetlana klawiatura
Czytnik linii papilarnych
Pojemność baterii minimum 41 Wh
System operacyjny Windows 11 Pro
Dodatkowe oprogramowanie Microsoft Office 2021 PL licencja wieczysta
Kolor czarny
Waga maksymalnie 1.70 kg
Zasilacz 65W
Gwarancja 3 lata naprawa NBD na miejscu użytkowania.