

Deduplikator sprzętowy do wykonywania kopii zapasowych – 1 sztuka

Nazwa komponentu	Opis Wymagań
Obudowa	Obudowa do montażu w szafie rack 19" za pomocą dostarczonych dedykowanych elementów.
Kontrolery	Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy zapisu i odczytu danych musi przejąć drugi kontroler.
Wydajność backupu	Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 4 TB/h (dane podawane przez producenta).
Wymagana przestrzeń	Przestrzeń całkowita musi składać się z min. 8 dysków NL-SAS po min. 4TB każdy. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS 12Gb/s o pojemności RAW pojedynczego dysku min 1,92TB jako cache pod zapis backupu. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń <i>spare</i> i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji. Urządzenie musi umożliwiać rozszerzenie posiadanej przestrzeni dyskowej przez dodawanie półek dyskowych do minimum 60 dysków HDD NL-SAS oraz 20 SSD SAS.
Zabezpieczenia RAID	Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 2 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-M poprzez mechanizm nadpisywania danych.
Pamięć Cache	Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.
Dostępne interfejsy	Urządzenie musi posiadać minimum: 8 x 1 Gb/s RJ45 , 4 x 10 Gb/s SFP+ z możliwością obsługi każdym portem Ethernet protokołów iSCSI, CIFS, NFS, wszystkie porty światłowodowe muszą być wyposażone we wkładki optyczne SR.
Obsługiwane protokoły	Wymagane wsparcie dla iSCSI, NFS, CIFS.
Zarządzanie	Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak: <ul style="list-style-type: none"> - cały deduplikator - kontrolery - CPU - porty front-end - porty logiczne - dyski - file systemy Pod kątem parametrów takich jak: <ul style="list-style-type: none"> - operacje wejścia/wyjścia IOPS - przepustowość (KB/s lub MB/s) - czas odpowiedzi (latency) - średnie użycie (w % dla CPU) Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego

	<p>serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.</p> <p>Wymagana możliwość monitorowania poboru prądu deduplikatora z rozbiem na miesiące oraz dni. Pobór prądu podawany w kWh.</p> <p>Wymagany dostęp do prognozy zużycia przestrzeni.</p> <p>Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>
Redukcja danych	<p>Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p> <p>Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci.</p> <p>Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych co najmniej 60:1</p>
Kontrola zasobów plikowych	<p>Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni.</p> <p>Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń.</p> <p>Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp.</p> <p>Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania.</p>
Ochrona zasobów plikowych	<p>Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system'ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.</p> <p>Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania.</p>
Replikacja danych	<p>Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję.</p>

	<p>Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00).</p> <p>Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączenie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania.</p> <p>Dostarczenie powyższych funkcjonalności nie jest wymagane na tym etapie postępowania.</p>
<p>Wspierane systemy backup</p>	<p>Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication, Bacula, Bareos.</p>
<p>Wbudowane oprogramowanie do backupu</p>	<p>Urządzenie musi posiadać wbudowane oprogramowanie do wykonywania kopii zapasowych i przywracania danych z kopii. zapasowej które pozwala wykorzystać przestrzeń dyskową urządzenia jako repozytorium danych.</p> <p>Oprogramowanie musi posiadać licencję pozwalającą na:</p> <ul style="list-style-type: none"> • Wykonywanie kopii zapasowych nielimitowanej liczby maszyn wirtualnych dla systemów wirtualizacji takich jak np. Vmware • Granulację backupu i odtwarzania na poziomie maszyny VM oraz pojedynczego dysku maszyny VM • Wykonywanie backupu w trybach pełnego, przyrostowego oraz w trybie „incremental forever” • Tworzenie zadań backupowych w oparciu o harmonogram • Tworzenie kopii systemów pliku dla Windows oraz Linux • Backup środowisk Vmware, Oracle, MySQL, DB2, SAP HANA, Windows • Pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
<p>Obsługa serwisowa</p>	<ol style="list-style-type: none"> 1) Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta na terenie RP. 2) Deduplikator musi zostać objęty minimum 60 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. 3) Uszkodzone dyski po awarii pozostają u Zamawiającego bez konieczności zwrotu do serwisu/producenta. 4) Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta. 5) Usługi gwarancyjne muszą być świadczone przez organizację serwisową producenta/producenta sprzętu posiadającą certyfikat ISO co najmniej 9001:2015. 6) Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: <ul style="list-style-type: none"> • możliwość pobierania najnowszego firmware; • dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń; • dostęp do centrum pomocy technicznej producenta; • otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware; • otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia

Macierz dyskowa - 2 szt.

Podać nazwę producenta i modelu

Nazwa komponentu	Wymagane minimalne parametry techniczne pojedynczej macierzy
Obudowa	Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19", dostarczone ze wszystkimi niezbędnymi komponentami do montażu. Wysokość dostarczonej macierzy musi wynosić maksymalnie 2U.
Kontrolery dyskowe	<p>Minimum dwa kontrolery macierzowe pracujące w trybie Symmetrical Active-Active/Mesh Active-Active, to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing) nawet dla pojedynczego LUN. W celu weryfikacji wymogu Zamawiający zastrzega możliwość wykonania testu w którym dla utworzonego jednego LUN operacje I/O muszą być realizowane jednocześnie przez porty w obu kontrolerach, a generowane obciążenie (IOPS oraz Bandwidth) mają być rozłożone dla pary kontrolerów w stosunku 50/50 +/- 10%. W przypadku zaoferowania większej ilości kontrolerów obciążenie ma być rozłożone proporcjonalnie na wszystkie kontrolery. Kontrolery muszą pozwalać na udostępnianie zasobów protokołami blokowymi. Komunikacja pomiędzy oferowanymi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband.</p> <p>Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze więcej niż 2 kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego.</p>
Możliwość rozbudowy	<p>Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 4 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązań opartych o wirtualizator.</p> <p>Macierz musi być skonstruowana wyłącznie do obsługi modułów pamięci SSD lub NVMe i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych.</p> <p>Urządzenie musi umożliwiać dynamiczną zmianę rozmiaru woluminów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się w danym LUN.</p> <p>Urządzenie musi umożliwiać rozbudowę przestrzeni dyskowej o pojedynczy dysk oraz pojedynczą półkę dyskową z możliwością rozszerzenia puli dyskowej o dodany dysk/półkę bez konieczności migracji danych ani zatrzymywania pracy macierzy.</p>
Wymagana przestrzeń	<p>Całkowita pojemność surowa RAW urządzenia musi wynosić minimum 46 TB i być zbudowana tylko i wyłącznie za pomocą dysków SSD lub NVMe o maksymalnej pojemności pojedynczego modułu 4 TB.</p> <p>Macierz musi umożliwiać rozbudowę do co najmniej 60 sztuk oferowanego typu dysków, bez wymiany lub dodawania kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek dyskowych oraz kart z interfejsami).</p> <p>Dyski muszą posiadać redundantne interfejsy SAS lub PCIe(dla NVMe).</p>

<p>Procesory/Pamięć Cache</p>	<p>Każdy kontroler macierzy musi być oparty o wielordzeniowe procesory, minimum dziesięć rdzeni na kontroler.</p> <p>Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.</p>
<p>Zabezpieczenie danych</p>	<p>Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.</p> <p>Urządzenie musi obsługiwać poziomy RAID5, RAID6 lub DP (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare), oraz RAID 10.</p>
<p>Dostępne interfejsy</p>	<p>Macierz musi posiadać:</p> <ul style="list-style-type: none"> • minimum 12 portów 10Gb/s obsługujących protokół iSCSI na całą macierz. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+/SFP28), wymaga się ich dostarczenia wraz z urządzeniem; <p>W oferowanej konfiguracji portów macierz musi posiadać pełną możliwość rozbudowy do wymaganej ilości modułów SSD bez usuwania żadnego z interfejsów.</p>
<p>Brak pojedynczego punktu awarii</p>	<p>Wszystkie krytyczne komponenty takie jak adaptory HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienne w trakcie pracy.</p>
<p>Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning)</p>	<p>Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation).</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>
<p>Protokoły dostępu do danych</p>	<p>Wymagane wsparcie dla protokołów FC oraz iSCSI.</p>
<p>Snapshoty</p>	<p>Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego woluminu LUN oraz minimum 1000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write).</p> <p>Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie wielu wolumenów naraz tj. tworzenie kopii zapasowej wielu LUNów jednocześnie</p> <p>Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii).</p> <p>Rozwiązanie musi umożliwiać stworzenie harmonogramu wykonywania kopii migawkowych w trybie „immutable” tj. kopii których przez zadany okres czasu (od 1 dnia do 12 miesięcy) nie można usunąć ani zmodyfikować w celu ochrony danych np. przed atakiem ransomware.</p>

	<p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania dla danych blokowych.</p>
Funkcje kopiujące	<p>Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>
Redukcja danych	<p>Macierz musi mieć funkcjonalność deduplikacji i kompresji danych w trybie in-line zarówno dla danych blokowych jak i systemu plików. Administrator musi mieć możliwość wyłączenia mechanizmów redukcji danych dla poszczególnych woluminów LUN.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie nie jest wymagane na tym etapie postępowania.</p>
Replikacja danych	<p>Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub IP bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznej macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>
Klaster wysokiej dostępności	<p>Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub IP pomiędzy 2 macierzami dostarczonymi w tym postępowaniu. Pod użytym 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. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać klastrowanie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>

Priorytety zadań	<p>Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS).</p> <p>Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>
Kompatybilność	<p>Model oferowanej macierzy musi wspierać systemy Windows Server, Vmware, RedHat oraz Proxmox.</p>
Wielosieczkowość	<p>Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows Server 2019 oraz 2022, Vmware 8.0 i nowszych.</p>
Zasilanie	<p>Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap.</p>
Zarządzanie macierzą	<p>Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności dysków SSD. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI z co najmniej 1 rok wstecz.</p> <p>Macierz musi umożliwiać monitorowanie oraz przeglądanie danych historycznych z podziałem dla każdego z LUN dla min. operacji:</p> <ul style="list-style-type: none"> -% trafień w cache do odczytu oraz zapisu -IOPS -średni czas odpowiedzi dla odczytu danych -średni czas odpowiedzi dla zapisu danych -przepustowość „Bandwidth” dla operacji odczytu -przepustowość „Bandwidth” dla operacji zapisu <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p> <p>Rozwiązanie musi udostępniać interfejs REST API w celu uruchamiania skryptów oraz SNMP do komunikacji z zewnętrznymi narzędziami monitorującymi.</p>
Serwisowalność	<p>Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.</p> <p>Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.</p> <p>Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną.</p>
Gwarancja, wsparcie serwisowe	<p>7) Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta na terenie RP.</p> <p>8) Macierz dyskowa musi zostać objęta minimum 60 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki.</p>

- | | |
|--|---|
| | <p>9) Uszkodzone dyski po awarii pozostają u Zamawiającego bez konieczności zwrotu do serwisu/producenta.</p> <p>10) Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta.</p> <p>11) Usługi gwarancyjne muszą być świadczone przez organizację serwisową producenta sprzętu posiadającą certyfikat ISO co najmniej 9001:2015.</p> <p>12) Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:</p> <ul style="list-style-type: none">• możliwość pobierania najnowszego firmware;• dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń;• dostęp do centrum pomocy technicznej producenta;• otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware;• otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy |
|--|---|

Serwery - 2 szt.

Podać nazwę i model

Nazwa komponentu	Wymagane minimalne parametry techniczne jednego serwera
Obudowa	Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 2,5". Wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie rack i wysuwanie serwera do celów serwisowych, z ramieniem do zarządzania przewodami oraz przednim panelem zamykanym na klucz, chroniącym dyski przed nieuprawnionym wyjęciem.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych.
Procesor	Zainstalowane dwa procesory 8-rdzeniowe o taktowaniu min. 2.8GHz (base frequency), umożliwiające osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 25 000 pkt. Testy dla oferowanego modelu procesora muszą być opublikowane i ogólnie dostępne na stronie https://www.cpubenchmark.net/high_end_cpus.html
Pamięć RAM	Minimum 384 GB RAM DDR4 RDIMM 4800MT/s, w modułach po 32 GB RAM. Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, patrol scrubbing, SDDC, memory thermal throttling, ADDDC-SR, PPR, Memory SMBus hang recovery.
Pamięć masowa	<ul style="list-style-type: none">zainstalowane 2 dyski serwerowe SSD SATA o pojemności min. 480 GB każdy,dyski typu 2,5" Hot-Plug. Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie RAID: 0, 1, 5, 6, 10, 50, 60.
Wbudowane porty	4 x USB z czego nie mniej niż 2 x USB (z czego min. 1x USB 3.0) oraz USB TYP-C na przednim panelu obudowy i 2 x USB 3.0 na tylnym panelu obudowy. 1 x VGA na tylnym panelu obudowy. Złącze USB TYP-C na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
Interfejsy sieciowe	Zainstalowane i w pełni funkcjonalne interfejsy: <ul style="list-style-type: none">minimum 1 x RJ-45 Ethernet management port,minimum 2 karty każda wyposażona w 2 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ 10Gb/s Multimode, karty nie mogą zajmować slotów PCI-Eminimum 2 karty zainstalowane w slotach PCI-E, każda wyposażona w 2 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ 10Gb/s Multimode
Sloty PCI-E	Minimum 3 aktywne sloty PCI-E 5.0, z czego jeden slot x16 oraz dwa sloty x8. Możliwość rozbudowy o dodatkowe 3 sloty PCI-E 5.0 x16.

Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wentylatory	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
Zasilanie	Minimum dwa identyczne zasilacze klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie więcej niż 1600W.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta. Moduł TPM 2.0.
Diagnostyka	Serwer wyposażony w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający: <ul style="list-style-type: none"> • wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS • wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy • przywracanie konta administratora • wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera • wyświetlanie w czasie rzeczywistym temperatury procesorów • konfigurowanie ustawień sieciowych modułu zarządzania.
Zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca: <ul style="list-style-type: none"> • monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), • monitorowanie w czasie rzeczywistym poboru prądu przez serwer, • zbieranie logów błędów hardware, • przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, • montowanie wirtualnych napędów, • zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, • wysyłanie zawiadomień drogą mailową i poprzez SNMP • wsparcia dla IPMI, SSH, Redfish • wsparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows, • nadawanie ról użytkownikom, • możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD, • możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.
Dodatkowe oprogramowanie do zarządzania i monitorowania	Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:

	<ul style="list-style-type: none"> • włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejście pełnej konsoli graficznej serwerów. • tworzenie szablonów instalacyjnych dla systemów operacyjnych. • tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów. • zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera. • aktualizacja sterowników i BIOS serwerów. • zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
Kompatybilność	<p>Zgodność z normą ISO 9001 oraz ISO 14001 lub równoważnymi.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów , Microsoft Windows Server 2022.Kompatybilność z VMware.</p>
Gwarancja	<ol style="list-style-type: none"> 1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP. 2. Urządzenie objęte minimum 60 miesięcznym okresem gwarancji w trybie 9x5 NBD onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. 3. Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta. 4. W przypadku awarii, uszkodzone dyski, pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention. 5. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny. 6. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: <ul style="list-style-type: none"> • możliwość pobierania najnowszego firmware, • dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń, • dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta, • otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
Licencje	<p>Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie minimum sześć instancji wirtualnych tego serwerowego systemu operacyjnego.</p> <p>Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.</p>

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:
 - pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - 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:
 - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - 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:
 - Login i hasło,
 - Karty z certyfikatami (smartcard),

- 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:
 - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - 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.
- Zdalna dystrybucja oprogramowania na stacje robocze.
- Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
- 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.
- Szyfrowanie plików i folderów.
- Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

- Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - Serwis udostępniania stron WWW.
 - Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - Wsparcie dla algorytmów Suite B (RFC 4869),
 - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 - 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. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

System Wirtualizacji – 1 komplet licencji

Podać nazwę oferowanego systemu:

Wymagania Minimalne	
1.	Licencja producenta na oprogramowanie wirtualizacyjne dla 2 serwerów łącznie posiadających 4 procesory. Możliwość rozbudowy klastra do 2000 serwerów.
2.	Licencja wieczysta pozwalająca na legalne używanie oprogramowania również w przypadku braku wykupienia usługi wsparcia u producenta. Zamawiający nie dopuszcza zaoferowania licencji w modelu subskrypcyjnym.
3.	Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
4.	Rozwiązanie musi zapewniać możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym.
5.	Oprogramowanie do wirtualizacji musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi, zasobami i warstwą sieciową na wszystkich hostach. Konsola powinna być możliwa do zainstalowania na niezależnej maszynie fizycznej.
6.	Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi obsłużyć i wykorzystać procesory fizyczne posiadające od 8 do 96 rdzeni.
7.	Oprogramowanie do wirtualizacji musi mieć możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych(vCPU).
8.	Oprogramowanie do wirtualizacji musi mieć możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
9.	Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
10.	Rozwiązanie musi być niezależne od producenta platformy sprzętowej.
11.	Rozwiązanie musi umożliwiać utworzenie maszyn wirtualnych na których będą uruchomione następujące systemy operacyjne: Windows Server 2019, Windows Server 2022, Windows Server 2016, SUSE Linux Enterprise Server 15, SLES 11, Ubuntu Server, Rocky Linux , RHEL 7, RHEL 8, RHEL9, Debian, CentOS.
12.	Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera.
13.	Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
14.	Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
15.	Rozwiązanie musi posiadać możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne z okresu 1 rok wstecz.
16.	Oprogramowanie do wirtualizacji musi posiadać możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17.	Oprogramowanie do wirtualizacji musi mieć możliwość klonowania maszyn VM wraz z ich pełną konfiguracją i danymi oraz umożliwiać modyfikację parametrów nowej maszyny która powstanie po operacji klonowania.
18.	Oprogramowanie do wirtualizacji wraz z systemem zarządzania musi mieć możliwość integracji z usługami katalogowymi Microsoft Active Directory poprzez szyfrowany protokół LDAP over SSL (LDAPS) .
19.	Rozwiązanie musi posiadać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn.
20.	Oprogramowanie do wirtualizacji musi obsłużyć przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.

21. Oprogramowanie do wirtualizacji musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
22. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi na których pracują. Mechanizm musi umożliwiać co najmniej 4 procesy przenoszenia jednocześnie.
23. Oprogramowanie do wirtualizacji musi zapewniać funkcjonalność HA zapewniającą automatyczną migrację maszyn wirtualnych pomiędzy serwerami bez przerywania pracy użytkowników lub ograniczenia dostępności usługi przy awarii jednego z hostów.
24. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy dyskami fizycznymi serwerów i/lub wolumenami macierzy na których znajdują się pliki, z których składa się wirtualna maszyna.
25. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
26. Pojedynczy wirtualny przełącznik musi mieć możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
27. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny musi mieć możliwość konfiguracji 4000 portów.
28. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
29. Wirtualny przełącznik musi posiadać następujące możliwości: <ul style="list-style-type: none"> – Agregacja portów: Możliwość agregacji indywidualnych portów na danym hoście (serwerze) do pojedynczej wiązki logicznej, zgodnie z protokołem LACP, – QoS: Traffic Shaping; – Zarządzanie: Zarządzanie wirtualnym przełącznikiem złożonym z wirtualnych modułów liniowych znajdujących się w hostach (serwerach) – VLAN;
<p>Gwarancja i wsparcie:</p> <p>W ramach usługi wsparcia technicznego dla Oprogramowania, Zamawiającemu przysługuje, przez okres co najmniej 60 miesięcy:</p> <ul style="list-style-type: none"> • prawo do korzystania, bez jakichkolwiek dodatkowych opłat z wydawanych przez producenta oprogramowania najnowszych jego wersji, aktualizacji oprogramowania, poprawek do oprogramowania; • zdalny dostęp elektroniczny przez całą dobę i wszystkie dni w roku (7X24) do Centrum Pomocy Technicznej producenta, z czasem podjęcia naprawy nie przekraczającym jednego dnia roboczego od momentu zgłoszenia problemu, a dla zgłoszeń krytycznych z czasem reakcji poniżej dwóch godzin; • zdalny dostęp elektroniczny do bazy wiedzy, dokumentacji, biuletynów i informacji na temat oprogramowania; • Nielimitowana liczba zgłoszeń serwisowych przez cały okres trwania wsparcia • możliwość zgłaszania problemów telefonicznie w języku polskim lub angielskim oraz za pośrednictwem e-mail <p>Licencja i oprogramowanie musi być nowe, nieużywane, nigdy wcześniej nieaktywowane. Zamawiający zastrzega sobie możliwość sprawdzenia legalności licencji u producenta oprogramowania.</p>