

Załącznik nr 1b do SWZ

Macierz dyskowa

Producent:

Model:

Ilość: 1 szt.

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U oraz możliwością instalacji min. 24 dysków 2.5"	
Przestrzeń dyskowa	Zainstalowane: - 12x dysków SAS o pojemności min. 2.4TB, Hot-Plug	
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardej.	
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".	
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).	

	Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.	
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.	
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.	
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.	
Interfejsy	Macierz musi posiadać, co najmniej 8 portów SAS 12Gb (4 porty na kontroler)	
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.	
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	

<p>Thin Provisioning</p>	<p>Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.</p> <p>Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>	
<p>Tiering</p>	<p>Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.</p> <p>Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.</p> <p>Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.</p>	
<p>Wewnętrzne kopie migawkowe</p>	<p>Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.</p> <p>Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>	
<p>Wewnętrzne kopie pełne</p>	<p>Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>	

<p>Migracja danych w obrębie macierzy</p>	<p>Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.</p>	
<p>Podłączanie zewnętrznych systemów operacyjnych</p>	<p>Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).</p> <p>Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.</p> <p>Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.</p>	
<p>Redundancja</p>	<p>Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.</p> <p>Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.</p> <p>Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik</p>	



	<p>zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.</p> <p>Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.</p>	
Dodatkowe wymagania	<p>Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.</p> <p>Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.</p>	
Standardy bezpieczeństwa	<p>Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)</p>	
Oprogramowanie	<p>Oparta na chmurze aplikacja która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none">• Monitoring:<ul style="list-style-type: none">○ ilość podłączonych oraz rozłączonych systemów○ stan podłączonych urządzeń○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia○ informacje o statusie gwarancji dla poszczególnych urządzeń○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy	



	<p>wykorzystania przestrzeni na pamięciach masowych.</p> <ul style="list-style-type: none">○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemu pamięci masowych.○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.○ Monitoring parametrów serwerów z informacją o minimum:<ul style="list-style-type: none">▪ Obciążeniu procesora▪ Zużyciu pamięci RAM▪ Temperaturze procesorów▪ Temperaturze powietrza wlotowego▪ Zużyciu prądu▪ Zmianach w fizycznej konfiguracji serwera▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.○ Monitoring parametrów pamięci masowych z informacją o minimum:<ul style="list-style-type: none">▪ Opóźnieniach▪ IOPS	
--	---	--



	<ul style="list-style-type: none">▪ Przepustowości▪ Utylizacji kontrolerów▪ Pojemność całkowita i dostępna▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata▪ Informacje o poziomie redukcji danych▪ Informacje o statusie replikacji oraz snapshotów○ Monitoring parametrów przełączników sieciowych z informacją o minimum:<ul style="list-style-type: none">▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny▪ Stanie komponentów: zasilacze, wentylatory▪ Podłączonych hostach▪ Ilości i statusu portów▪ Utylizacji procesora▪ Utylizacji poszczególnych portów▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.	
--	--	--

- Aktualizacja firmware



- możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
 - Możliwość generowania raportów dla serwerów zawierających informację o:
 - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
 - Średnim obciążeniu: procesorów, pamięci RAM, IO,
 - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
 - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o

	<p>utworzonych LUN-ach i systemach pliku, status replikacji</p> <ul style="list-style-type: none">○ Generowanie raportów do plików CSV i PDF● Cyberbezpieczeństwo<ul style="list-style-type: none">○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urzędzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urzędzeń.○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.● Wspierane urzędzenia<ul style="list-style-type: none">○ Urzędzenie Producenta dostarczane w ramach postępowania○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urzędzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;● Możliwość rozszerzenia funkcjonalności<ul style="list-style-type: none">○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.● Inne<ul style="list-style-type: none">○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android● Certyfikaty	
--	---	--

	<ul style="list-style-type: none"> ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: <ul style="list-style-type: none"> ▪ ISO 27001 ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization <p>CSA Cloud Control Matrix</p>	
<p>Inne</p>	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane jest aby macierz została wyprodukowana zgodnie z normami ISO 9001 oraz ISO 14001.</p> <p>Deklaracja zgodności CE.</p>	
<p>Warunki gwarancji</p>	<p>Min. 24 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</p> <p>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</p>	



Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.

Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.

Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.

Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Możliwość rozszerzenia gwarancji przez producenta do 5 lat.

Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty.

Wskazana firma serwisująca musi posiadać autoryzację producenta urządzenia – na potwierdzenie należy załączyć ogólnodostępny link do strony producenta urządzenia z ogólnodostępnym dokumentem np. certyfikat lub deklaracja producenta, potwierdzającym autoryzację dla firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku braku takiego linku lub ogólnodostępnego dokumentu producenta, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firmy serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski.