



KATOWICKIE CENTRUM ONKOLOGII

UL. RACIBORSKA 26 40 - 074 K A T O W I C E

NIP 634-22-99-376 REGON 276201240

tel. 32 42 00 100

fax. 32 25 14 533

e-mail: szpital@kco.katowice.pl



Katowice, dnia 27.01.2021 r.

KCO/AT/ZL/ZP/JW/ 91./2021

Dotyczy: przetargu nieograniczonego o wartości szacunkowej zamówienia powyżej 214 000 euro na zakup, dostarczenie i montaż wyposażenia serwerowni dla Katowickiego Centrum Onkologii
Znak sprawy: K.C.O./PN/62/2020

I. ODPOWIEDZI NA PYTANIA DO SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Zamawiający – Katowickie Centrum Onkologii, informuje, że do specyfikacji istotnych warunków zamówienia wpłynęły następujące pytania:

Pytanie nr 1 Dotyczy pkt. 40 OPZ do Pakietu 5.

„Użyteczność oraz dojrzałość technologiczna zaoferowanego rozwiązania musi być potwierdzona obecnością producenta rozwiązania w Magicznym Kwadrancie Gartnera (MQ) dla Security Information and Event Management (SIEM) z 2020 roku.” Na rynku istnieją rozwiązania, które realizują wymagania stawiane przed nimi w ramach przedmiotowego postępowania, ale nie są one obecne w rankingach takich jak Magiczny Kwadrant Gartnera czy Forrester. Dotyczy to chociażby polskich producentów rozwiązań klasy SIEM, którzy ze względów czysto finansowych nie są w stanie używać tego typu narzędzi marketingowych. Należy pamiętać, że powyższe rankingi mają obecnie głównie charakter marketingowy i nie powinno się ich traktować jako narzędzie do weryfikacji dojrzałości rozwiązań informatycznych. W związku z powyższym wnosimy o usunięcie zapisu z SIWZ jako rażąco ograniczającego konkurencję w niniejszym postępowaniu uniemożliwiającego start w postępowaniu między innymi krajowym producentom.

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Pytanie nr 2 Pytania dotyczą pakietu nr 1 - Zdalne Zarządzanie.

Zbiór opisanych parametrów skazuje jednoznacznie na rozwiązanie Dell R740. Wnosimy o dopuszczenie równoważnego rozwiązania charakteryzującego się poniższymi parametrami:

Niezależna od system operacyjnego, posiadająca funkcjonalność:

- monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne)
- wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
- dostęp do karty zarządzającej poprzez
 - dedykowany port RJ45 z tyłu serwera lub
 - przez współdzielony port zintegrowanej karty sieciowej serwera



Śląskie.

Jednostka ochrony zdrowia Samorządu Województwa Śląskiego.

- dostęp do karty możliwy
 - z poziomu przeglądarki internetowej (GUI)
 - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
 - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
- wbudowane narzędzia diagnostyczne
- zdalna konfiguracja serwera (BIOS) i instalacji systemu operacyjnego
- obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
- wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
- przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
- obsługa zdalnego serwera logowania (remote syslog)
- wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
- funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy)
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
- zdalna aktualizacja oprogramowania (firmware)
- zarządzanie grupami serwerów, w tym:
 - tworzenie i konfiguracja grup serwerów
 - sterowanie zasilaniem (wł/wył)
 - ograniczenie poboru mocy dla grupy (power capping)
 - aktualizacja oprogramowania (firmware)
 - wspólne wirtualne media dla grupy
- możliwość równoczesnej obsługi przez min. 2 administratorów
- autentykacja dwuskładnikowa (Kerberos)
- wsparcie dla Microsoft Active Directory
- obsługa TLS i SSH
- możliwość trwałego zablokowania dokonania obniżenia wersji oprogramowania układowego (firmware) serwera
- wsparcie dla algorytmów CNSA
- wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API
- możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Pytanie nr 3 Dot. Wsparcia dla systemów operacyjnych i systemów wirtualizacyjnych.

Zamawiający wymaga dostarczenia najnowszych rozwiązań technologicznych jednocześnie wymagając wsparcia dla systemów firmy Microsoft, które od kilku lat są niewspierane przez producenta i są źródłem wielu ataków cybernetycznych.

Jednocześnie należy zauważyć, że wymagane wsparcie posiada ww. Dell R740

PowerEdge R740
by Dell Inc

Windows Server 2019 Certified
Windows Server 2016 Certified
Windows Server 2012 R2 Certified
Windows Server 2012 Certified

Compatible with the following versions of Microsoft Windows

	Windows Server 2019 x64	Certified for Windows <ul style="list-style-type: none"> • Hardware Assurance • NV-DIMM-I Capable • Software-Defined Data Center (SDDC) Premium
	Windows Server 2016 x64	Certified for Windows <ul style="list-style-type: none"> • Hardware Assurance • Software-Defined Data Center (SDDC) Premium
	Windows Server 2012 R2 x64	Certified for Windows
	Windows Server 2012 x64	Certified for Windows

View submission details for a compatible operating system:

(select a compatible Windows version)

Wnosimy o dopuszczenie najnowszych rozwiązań serwerowych posiadających wsparcie dla poniższych systemów:

Microsoft Windows Server 2016,2019

Red Hat Enterprise Linux (RHEL) 7.X lub nowszy

SUSE Linux Enterprise Server (SLES) 12 lub nowszy

VMware ESXi 6.5 U1 lub nowszy.

Dopuszczenie powyższych zmian pozwoli zaoferować Zamawiającemu wysokiej klasy rozwiązania innych firm niż Dell i zachować ramy konkurencyjności co jest wymagane przez Prawo Zamówień Publicznych.

Odpowiedź:

Zamawiający dopuszcza takie rozwiązanie.

Pytanie nr 4 Dot. Pakiet 2

Zbiór opisanych przez Zamawiającego wymagań wskazuje jednoznacznie na macierz firmy Dell model ME4084.

W związku z tym, że Zamawiający finansuje zakup ze środków publicznych wnosimy o zachowanie wytycznych PZP i dopuszczenie rozwiązań konkurencyjnych a nie blokowanie możliwości złożenia konkurencyjnej oferty tylko przez partnerów firmy Dell.

Wnosimy o dopuszczenie rozwiązania macierzowego innego producenta o poniższych parametrach (rozwiązanie te jest rozwiązaniem równoważnym do wymagań określonych przez Zamawiającego w OPZ):

L.p.	Cecha	Wymagania minimalne
1.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19".

2.	Przestrzeń dyskowa	<p>Macierz musi być wyposażona w co najmniej:</p> <p>10 dysków 2,5" HotPlug SSD: typu co najmniej Mix Use o pojemności co najmniej 1,6TB, SAS, 12Gb/s;</p> <p>10 dysków 2,5" HotPlug SSD: typu co najmniej Mix Use o pojemności co najmniej 1,9TB, SAS, 12Gb/s; 18 dysków 2,5" HotPlug SAS 12Gb o pojemności co najmniej 1.8TB, 10k rpm.</p> <p>Dodatkowe moduły dyskowe (półki dyskowe) z możliwością zainstalowania co najmniej 60 dysków 3,5" zawierające co najmniej:</p> <p>28 dysków 3,5" HotPlug o pojemności co najmniej 6TB NLSAS 12Gb/s, 7.2k rpm.</p> <p>29 28 dysków 3,5" HotPlug o pojemności co najmniej 8TB NLSAS 12Gb/s, 7.2k rpm</p>
3.	Możliwość rozbudowy	<p>Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 220 dysków twardech.</p> <p>Macierz musi umożliwiać zwiększenie pojemności użytkowej poprzez dodanie pojedynczego dysku bez zmiany istniejącego poziomu zabezpieczenia RAID oraz bez utraty dostępu do danych.</p>
4.	Obsługa dysków	<p>Macierz musi obsługiwać dyski SSD, SAS i NL SAS. Macierz musi obsługiwać dyski 2,5" jak również 3,5".</p>
		<p>Komunikacja z dyskami 12Gb SAS.</p>
5.	Sposób zabezpieczenia danych	<p>Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardech (tzw. widestriping).</p> <p>Jeżeli funkcjonalność tzw. wide-striping w oferowanej macierzy nie jest dostępna to należy wyposażyć macierz w 50% więcej przestrzeni dyskowej brutto dla każdego typu dysków wymienionych w punkcie „Przestrzeń dyskowa”. Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków.</p>
6.	Tryb pracy kontrolerów macierzowych	<p>Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC 16Gb. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC.</p>
7.	Pamięć cache	<p>Każdy kontroler macierzowy musi być wyposażony w minimum 12GB pamięci Cache, 24 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.</p> <p>Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.</p> <p>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.</p>
8.	Rozbudowa pamięci cache	<p>Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.</p> <p>Należy dostarczyć 64 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 128GB).</p>



9.	Rozbudowa pamięci cache (punktowane – 2 pkt.)	Dostarczenie macierzy z 128 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 256GB).
10.	Interfejsy do hostów	Macierz musi posiadać, co najmniej 8 portów FC 16Gb obsadzone wkładkami SFP SW 16 Gb/s.
11.	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. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: <ul style="list-style-type: none"> • administrator – pełen dostęp, monitor – możliwość odczytu konfiguracji.
12.	Kreator konfiguracji	System zarządzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy.
13.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Możliwość tworzenia wolumenów logicznych o pojemności maksymalnej co najmniej 140TB. 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 funkcjonalność tzw. wide-striping w oferowanej macierzy nie jest dostępna to należy wyposażyć macierz w 50% więcej przestrzeni dyskowej brutto dla każdego typu dysków wymienionych w punkcie „Przestrzeń dyskowa”.
14.	Szyfrowanie	Macierz musi umożliwiać szyfrowanie zapisywanych na niej danych. Nie wymaga się tej funkcjonalności w chwili dostawy.
15.	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning.
		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). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16.	Wewnętrzne kopie migawkowe	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.


Śląskie.

Jednostka ochrony zdrowia Samorządu Województwa Śląskiego.

		Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
17.	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
18.	Migracja danych w obrębie macierzy	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. 2 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 urządzenia.
19.	Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
20.	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware. 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. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
21.	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
22.	Migracja danych w obrębie macierzy	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. 2 typach dysków



Śląskie.

Jednostka ochrony zdrowia Samorządu Województwa Śląskiego.

		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 urządzenia.
23.	Redundancja	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. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
24.	Gwarancja	Macierz dyskowa objęta jest minimum 5 letnim okresem gwarancji producenta w miejscu instalacji z czasem reakcji serwisu najpóźniej na następny dzień roboczy od dnia zgłoszenia. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Uszkodzone dyski pozostają własnością Zamawiającego. Producent macierzy musi umożliwiać skuteczne usunięcie awarii wszystkich komponentów macierzy, włącznie z uszkodzonymi dyskami. Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą e-mail (w ofercie należy podać dedykowany adres e-mail serwisu producenta macierzy do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. Możliwość sprawdzenia statusu gwarancji i pełnej konfiguracji oferowanej macierzy na stronie producenta po podaniu nr seryjnego serwera.

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Zaproponowane przez Oferenta parametry są znacząco niższe od oczekiwanych, określonych projektem do którego urządzenie ma zostać wykorzystane, wnioskowana zmiana obniżyłaby oczekiwaną wydajność rozwiązania i funkcjonalność w odniesieniu do planowanego na przyszły rok II etapu rozbudowy środowiska Teleinformatycznego.

Pytanie nr 5

W wymaganiach dotyczących obudowy serwerów wirtualizacji Zamawiający wskazał: „Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą”. Wskazane wymaganie, w połączeniu z pozostałymi wymaganiami dotyczącymi serwerów wirtualizacji, spełnione jest wyłącznie przez jednego producenta rozwiązań serwerowych (DellEMC). Takie działanie świadczy o





faworyzowaniu konkretnego rozwiązania, co jest sprzeczne z Prawem Zamówień Publicznych. Prosimy zatem o zrezygnowanie z wymogu dostarczenia serwera z wbudowanym czujnikiem otwarcia obudowy. Zaznaczamy, iż wymaganie określone w obecnej formie narusza zasadę uczciwej konkurencji, równego traktowania wykonawców, przejrzystości i niedyskryminacji, co skutkuje - w przypadku projektów współfinansowanych ze środków UE - nałożeniem na Zamawiającego korekt finansowych (liczonych od całej wartości projektu, co stanowi wysokie kwoty pieniężne).

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Wymagany przez Zamawiającego czujnik otwarcia obudowy jest jednym z elementów bezpieczeństwa środowiska przetwarzania danych, który pozwala na zaalarmowanie administratora przy każdej próbie ingerencji w sprzęt przez osoby nieuprawnione, minimalizuje także ryzyko otwarcia niewłaściwego serwera przez serwisanta co jest istotne szczególnie w środowiskach, w których poszczególne elementy są dostarczone przez różnych dostawców.

Pytanie nr 6

W wymaganiach dotyczących kontrolera RAID w serwerach wirtualizacji Zamawiający wskazał: „Sprzętowy kontroler dyskowy posiadający min. 2GB nieulotnej pamięci cache”. Najczęściej stosowaną technologią zabezpieczania pamięci cache kontrolerów RAID przed utratą danych w przypadku awarii zasilania jest podtrzymanie bateryjne. Natomiast nieulotna pamięć cache typu NVDIMM w kontrolerach RAID wykorzystywana jest przez bardzo wąską grupę producentów rozwiązań serwerowych. Jednak mając na uwadze pozostałe zapisy dotyczące serwerów wirtualizacji, wymaganie to może być spełnione wyłącznie przez jednego producenta rozwiązań serwerowych (DellEMC). Takie działanie świadczy o faworyzowaniu konkretnego rozwiązania, co jest sprzeczne z Prawem Zamówień Publicznych. Prosimy zatem o dopuszczenie serwerów wyposażonych w podtrzymanie bateryjne pamięci cache kontrolerów RAID, w szczególności iż, oba rozwiązania zapewniają odpowiednio wysokie bezpieczeństwo danych. Pragniemy również zauważyć, że planowane wykorzystanie tych serwerów jako platformy wirtualizacyjnej przenosi ciężar zapewnienia najwyższego poziomu niezawodności na inne elementy infrastruktury. Zaznaczamy, iż wymaganie określone w obecnej formie narusza zasadę uczciwej konkurencji, równego traktowania wykonawców, przejrzystości i niedyskryminacji, co skutkuje - w przypadku projektów współfinansowanych ze środków UE - nałożeniem na Zamawiającego korekt finansowych (liczonych od całej wartości projektu, co stanowi wysokie kwoty pieniężne).

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Pytanie nr 7

W wymaganiach dotyczących zdalnego zarządzania serwerami wirtualizacji Zamawiający wskazał: „Możliwość zarządzania dostarczonymi serwerami z wykorzystaniem wdrożonego u Zamawiającego oprogramowania Openmanage Enterprise, lub dostarczenie alternatywnego rozwiązania o identycznej funkcjonalności, opisanego poniżej jako „Oprogramowanie alternatywne do zarządzania”) pod warunkiem wdrożenia dostarczonego rozwiązania i uruchomienia go dla posiadanych obecnie przez Zamawiającego urządzeń (serwery, macierze) - jeżeli spełnienie funkcjonalności wymaga dodatkowych pluginów i/lub licencji należy je dostarczyć w ramach postępowania”. Mimo, iż dopuszczone zostało oprogramowanie alternatywne, musi ono posiadać identyczne funkcjonalności jak oprogramowanie DellEMC OpenManage Enterprise i dodatkowo musi obsługiwać w pełnym zakresie urządzenia, które obecnie są w posiadaniu Zamawiającego, i które zarządzane są z użyciem oprogramowania DellEMC.



Tak postawione wymaganie nie jest możliwe do spełnienia przez jakiegokolwiek inne oprogramowanie niż DellEMC OpenManage, gdyż aplikacje do zarządzania wszystkich producentów mogą się integrować z urządzeniami firm trzecich wyłącznie za sprawą protokołu SNMP, przez który wysyłane są wyłącznie informacje o stanie urządzenia lub jego komponentów. Nie dają zatem możliwości zarządzania (zmiany parametrów, konfiguracji zabezpieczeń i ról użytkowników, itp.), a jedynie monitorowania. Tak postawione wymagania w tym postępowaniu uniemożliwiają zaoferowanie zarówno oprogramowania, jak i serwerów innych producentów jak DellEMC, co jest sprzeczne z Prawem Zamówień Publicznych. Prosimy zatem o dopuszczenie alternatywnego oprogramowania do zarządzania i monitorowania, które będzie współpracować z obecnie posiadanymi przez Zamawiającego urządzeniami (serwery, macierze) na zasadzie przechwytywania informacji wysyłanych przez nie za pomocą protokołu SNMP, oraz które będzie spełniać postawione wymagania dla alternatywnego oprogramowania do zarządzania, poza modulem raportującym. Zaznaczamy, iż wymaganie określone w obecnej formie narusza zasadę uczciwej konkurencji, równego traktowania wykonawców, przejrzystości i niedyskryminacji, co skutkuje - w przypadku projektów współfinansowanych ze środków UE - nałożeniem na Zamawiającego korekt finansowych (liczonych od całej wartości projektu, co stanowi wysokie kwoty pieniężne).

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Zamawiający zarządza całością infrastruktury teleinformatycznej samodzielnie i utrzymanie spójności zarządzania i serwisowania jest kluczowe, szczególnie w przypadku specyficznych potrzeb jakimi jest przetwarzanie i przechowywanie krytycznych danych związanych ze zdrowiem pacjentów.

Pytanie nr 8

W wymaganiach ogólnych dotyczących macierzy podstawowej Zamawiający wskazał: „Macierz posiadająca dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji co najmniej 30 dysków”, natomiast w dalszej części dotyczącej wymaganej przestrzeni dyskowej wyszczególnione jest 10 dysków SSD oraz 18 dysków SAS 12Gb, z zaznaczeniem, że: „Wszystkie powyższe dyski muszą zostać zamontowane w ramach jednostki głównej macierzy”. Wobec powyższego, Zamawiający wymaga, aby w jednostce kontrolerowej zainstalowane było 28 dysków, z dwoma dodatkowymi wnękami pustymi pod rozbudowę o kolejne dyski. Wskazane wymaganie spełnione jest wyłącznie przez jedną linię macierzową, a mianowicie Compellent, firmy Dell. Takie działanie świadczy o faworyzowaniu konkretnego rozwiązania, co jest sprzeczne z Prawem Zamówień Publicznych. Prosimy zatem o zrezygnowanie z wymagania dotyczącego minimalnej ilości dysków, jakie można zainstalować w jednostce kontrolerowej macierzy, bądź obniżenie wymagania z 30 szt. dysków, do 24 szt. dysków, co umożliwi zaoferowanie rozwiązań wielu wiodących producentów macierzy dyskowych. Zaznaczamy, iż wymaganie określone w obecnej formie narusza zasadę uczciwej konkurencji, równego traktowania wykonawców, przejrzystości i niedyskryminacji, co skutkuje - w przypadku projektów współfinansowanych ze środków UE - nałożeniem na Zamawiającego korekt finansowych (liczonych od całej wartości projektu, co stanowi wysokie kwoty pieniężne).

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Pytanie nr 9

W wymaganiach ogólnych dotyczących macierzy podstawowej Zamawiający wskazał: „Macierz musi umożliwiać rozbudowę o dodatkowe moduły dyskowe (poprzez dedykowane porty co najmniej 12 Gb

SAS na każdy kontroler): 12 dysków 3,5" o wysokości do 2U". Prosimy o dopuszczenie rozwiązania macierzowego, które umożliwi rozbudowę o dyski 3,5" w ramach półek dyskowych o wysokości 4U, mieszczących minimum 24 dyski formacie LFF. W przeliczeniu na wysokość Rack Unit, zaproponowane rozwiązanie będzie tożsame z pierwotnie postawionym wymaganiem, gdyż będzie umożliwiało zainstalowanie 12 dysków 3,5" w wysokości 2U.

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Pytanie nr 10

W wymaganiach dotyczących wymaganej przestrzeni w macierzy podstawowej Zamawiający wskazał: „co najmniej 10 dysków 2,5" HotPlug SSD: typu co najmniej Mix Use o pojemności co najmniej 1,6TB, SAS, 12Gb/s" oraz w dalszej części, jako wymaganie dodatkowo punktowane: „co najmniej 10 dysków 2,5" HotPlug SSD: typu co najmniej Mix Use o pojemności co najmniej 1,9TB, SAS, 12Gb/s". Prosimy o dopuszczenie zaoferowania sumarycznej przestrzeni w warstwie SSD SAS 12Gb/s, a więc odpowiednio dla wymagania podstawowego 16TB oraz dla wymagania dodatkowo punktowanego 19TB, z użyciem dysków o większej pojemności, np. 3,84TB. Zgodnie z zaproponowanym rozwiązaniem, Oferent zaoferuje minimum 9 dysków 3,84TB 2,5" SSD SAS 12Gb/s w ramach wymagania podstawowego oraz minimum 5 dysków 3,84TB 2,5" SSD SAS 12Gb/s w ramach wymagania dodatkowo punktowanego. Zwracamy uwagę, że zaoferowane ilości dysków zapewnią większą przestrzeń surową, niż obecnie Zamawiający wyszczególnił, co przełoży się na większą przestrzeń roboczą na dane produkcyjne. Dodatkowo, zaoferowane rozwiązanie macierzowe będzie korzystało z technologii RAID opartej na wirtualizacji przestrzeni na poziomie bloku, co zapewni nawet 20 razy szybsze czasy odbudowy danych, niż w tradycyjnej technologii RAID.

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Zamawiający nie wymaga dostarczenia dwóch rodzajów dysków.

Zamawiający uwzględnił również planowane potrzeby wydajnościowe jak i bezpieczeństwo danych, stąd ilość dysków – 8 „roboczych” oraz 2 HotSpare. Pojemność dysków została określona jako minimalna, więc dopuszczalne jest dostawa o większej pojemności jednak ze względu na konieczność zachowania wymaganej wydajności i poziomu bezpieczeństwa w planowanej konfiguracji w ilości 10 szt.

Pytanie nr 11

W wymaganiach dotyczących wymaganej przestrzeni w macierzy podstawowej Zamawiający wskazał: „Dodatkowy moduł dyskowy z możliwością zainstalowania co najmniej 60 dysków 3,5" zawierający”, m.in. dyski opisane następująco: „28 dysków 3,5" HotPlug o pojemności co najmniej 6TB NLSAS 12Gb/s, 7.2k rpm". Ze względu na różne konstrukcje stosowane przez producentów macierzy dyskowych, nie jest możliwe zaoferowanie przez wszystkich producentów dokładnie takich dysków, jak wskazane, w półkach dyskowych wysokiej gęstości. Prosimy by Zamawiający dopuścił zaoferowanie sumarycznej przestrzeni surowej w ramach powyżej wskazanego wymagania, z użyciem dysków o pojemności minimum 8TB. Zgodnie z zaproponowanym rozwiązaniem, Oferent zaoferuje minimum 21 dysków 8TB. Warto zaznaczyć, iż Zamawiający wymaga dostarczenia również „28 dysków 3,5" HotPlug o pojemności co najmniej 8TB NLSAS 12Gb/s, 7.2k rpm" w wymaganej półce wysokiej gęstości, co sprawia, że zaoferowane rozwiązanie będzie bardziej zunifikowane pod kątem dyskowym, a to przekłada się na uproszczone planowanie potencjalnych zapasów części zamiennych (dyski) oraz uproszczone czynności serwisowe.

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Zamawiający nie wymaga dostarczenia dwóch rodzajów dysków, tylko jednych lub drugich, Zamawiający uwzględnił w swoich potrzebach również dyski HotSpare, stąd wymagana ilość 28 dysków (w tym 4 dyski dedykowane jako hotspare), oraz możliwość rozbudowy/skalowalności dostępnej przestrzeni.

Pytanie nr 12

W wymaganiach dotyczących dostępności w macierzy podstawowej Zamawiający wskazał: „możliwość zastosowania RAID 10DM”. Tak postawione wymaganie jednoznacznie wskazuje na rozwiązanie jednego producenta, firmy Dell. Prosimy o zrezygnowanie z tego wymagania, w celu możliwości zaoferowania większej ilości konkurencyjnych rozwiązań macierzowych. Zaznaczamy, iż wymaganie określone w obecnej formie narusza zasadę uczciwej konkurencji, równego traktowania wykonawców, przejrzystości i niedyskryminacji, co skutkuje - w przypadku projektów współfinansowanych ze środków UE - nałożeniem na Zamawiającego korekt finansowych (liczonych od całej wartości projektu, co stanowi wysokie kwoty pieniężne).

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Pytanie nr 13 Dot. Zał. Nr 4 do SIWZ – IPU

W myśl par. 4 Zamawiający wymaga 24 rat, a tym samym 24 faktur z tytułu realizacji przedmiotu umowy. Z uwagi na przyjętą konstrukcję finansową, prosimy o informację, w którym momencie Zamawiający uznaje, iż dostarczony przedmiot umowy staje się jego własnością?

Odpowiedź:

W momencie zawarcia umowy.

Pytanie nr 14 Dot. Zał. Nr 4 do SIWZ – IPU

W myśl par. 6 Zamawiający przewiduje kary jedynie dla Wykonawcy. Biorąc pod uwagę ratalne płatności prosimy o przewidzenie w umowie kar umownych dla Zamawiającego z tytułu nieterminowej płatności dla Wykonawcy w wysokości 0,2% za każdy dzień opóźnienia.

Odpowiedź:

W każdym wypadku z tytułu zwłoki Zamawiającego w płatnościach, Wykonawcy przysługują odsetki za opóźnienie.

Pytanie nr 15 Dot. Zał. Nr 4 do SIWZ – IPU

Dot. Zał. Nr 4 do SIWZ – IPU – dotyczy zapisów par. 10 ust. 2 i 3. Prosimy o zamieszczenie zapisu umownego mówiącego o uregulowaniu przez Zamawiającego pozostałej płatności do końca trwania umowy w przypadku odstąpienia od umowy lub wypowiedzenia umowy z winy leżącej po stronie Zamawiającego.

Odpowiedź:

We wskazanej jednostce redakcyjnej brak zakresu odpowiadającego zapytaniu.

Pytanie nr 16 Pytanie 1 - Dot. Pakiet 1, „Karty rozszerzeń”

Zamawiający wymaga karty FC HBA dwu portowej o „łącznej przepustowości co najmniej 32Gbps”. Czy Zamawiający ma na myśli kartę dwu portową FC HBA, w której każdy port będzie miał przepustowość 16Gbps, co łącznie da nam 32Gbps ?

Odpowiedź:

Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Zamawiający wymaga karty dwu portowej FC HBA, w której każdy port będzie miał przepustowość 16Gbps, co łącznie pozwoli uzyskać 32Gbps.

Pytanie nr 17 Dot. Pakiet 2, „Wymagana przestrzeń”

Zamawiający wymaga łącznie 28 dysków (10szt. SSD 1.6TB lub 1.9TB SSD oraz 18szt. 2.5” 1.8TB SAS) zamontowanych w ramach „jednostki głównej macierzy”. Prosimy o potwierdzenie, że Zamawiający poprzez termin „jednostki głównej macierzy” ma na myśli jednostkę główną macierzy wyposażoną w dwa kontrolery w jednej obudowie, nie wliczając w tym żadnych półek dyskowych.

Odpowiedź:

Tak. Zgodnie z Załącznikiem nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

Pytanie nr 18 Dot. Pakiet 2 „Interfejsy zewnętrzne”

Zamawiający wymaga, aby „każdy kontroler był wyposażony co najmniej w 4 porty FC 32Gb/s oraz 1 port zarządzający 1GbE Base-T”. Poniżej Zamawiający zawarł zapis dodatkowo punktowany „Każdy kontroler musi być wyposażony w dodatkowe 4 porty FC 32Gb/s (SFP+) lub 4 porty SFP28 z wkładkami 25Gb wspierające obsługę protokołu iSCSI”

Prosimy o potwierdzenie, że warunki minimalne oraz dodatkowo punktowane będą spełnione, jeśli zostanie zaoferowana macierz z dwoma kontrolerami, w którym każdy kontroler będzie wyposażony w 4 porty FC 32Gb/s i 1 port zarządzający 1GbE Base-T oraz dodatkowe 4 porty FC 32Gb/s, czyli sumarycznie po 8 portów FC 32Gb/s (SFP+) i 1 port zarządzający 1GbE Base-T per kontroler.

Odpowiedź:

Tak.

Pytanie nr 19 Dotyczy wymagania 23 do pakietu 5

"SIEM umożliwi eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML. "

Zwracamy się z pytaniem, czy dla zadania eksportu i importu danych akceptowalnym formatem zapisu może być JSON. Podkreślamy, że proces eksportu i importu dashboardów jest procesem wewnętrznym aplikacji i nie wymaga udziału użytkownika ani znajomości tego formatu przez niego.

Odpowiedź:

SIEM umożliwi eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML.”

Zamawiający w celu standaryzacji oraz bacząc na użyteczność i łatwość edycji preferuje format XML który punktuje dodatkowo. W przypadku zaoferowania innego formatu danych Oferent nie otrzyma punktu jednak oferta nie zostanie odrzucona. Jest to wymóg stanowiący pozacenowe kryteria wyboru oferty.

Pytanie nr 20 Dotyczy wymagania 28.1 do pakietu 5

"System musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adres MAC, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji. "

Czy dla procesu anonimizacji danych akceptowalnym rozwiązaniem będzie mechanizm blokowania widoczności wskazanych pól dla użytkowników pracujących we wskazanych rolach ? Zwracamy jednocześnie uwagę, że wymagany proces anonimizacji według założeń SIWZ, nie jest poprawną anonimizacją danych, ponieważ zakłada odwrotne działanie tego procesu. Zaleceniem jest zastosowanie

kontroli bezpieczeństwa dla pól oraz anonimizacja jednokierunkowa, bez możliwości wtórnego odtworzenia oryginalnych danych.

Odpowiedź:

System musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adres MAC, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji. "

Zamawiający jest przekonany, iż zubażanie danych zaburza raportowanie i statystyki gdyż dane dot. niektórych ataków jak na przykład BruteForce mogą nie zostać poprawnie zidentyfikowane przez określone reguły. Anonimizacja jednokierunkowa w przypadku systemu nadzorującego bezpieczeństwo sieciowe może wpłynąć na czas reakcji w przypadku zdarzenia wymagającego szybkiej reakcji zespołu ds. bezpieczeństwa informatycznego. W przypadku zaoferowania innego sposobu anonimizacji lub jej braku Oferent nie otrzyma punktu jednak oferta nie zostanie odrzucona. Jest to wymóg stanowiący pozacenowe kryteria wyboru oferty.

Pytanie nr 21

Proszę o odpowiedź na pytanie, czy Zamawiający posiada już w swojej infrastrukturze oprogramowanie do Backupu, jeśli tak proszę o informację jakie licencje i ile szt. ?

Jeśli Zamawiający posiada już licencje oprogramowania do backupu i w ramach postępowania zakupi licencje oprogramowania tego samego producenta, to będzie istniała możliwość uzyskania korzystniejszych cen na licencje oprogramowania backupowego w ramach pakietu 4.

Odpowiedź:

Zamawiający posiada i wykorzystuje oprogramowanie różnych producentów. Na etapie postępowania nie możemy określić jakie oprogramowanie zostanie zaoferowane.

W załączeniu:

1. Zmiana SIWZ z dnia 25.01.2021r. – strona 10, strona 11
2. Załącznik nr 2 do SIWZ po zmianie z dnia 25.01.2021r.

II.

ZMIANA TERMINU SKŁADANIA I OTWARCIA OFERT

Zamawiający – Katowickie Centrum Onkologii przedłuża termin składania ofert **do dnia 15.02.2021r. do godz. 10:00.**

Oferty należy złożyć za pośrednictwem Platformy zakupowej e-Zamawiający (Marketplanet).

Otwarcie ofert nastąpi w dniu **15.02.2021r. o godz. 12:00** w Sekcji Zamówień Publicznych w Katowicach przy ul. Raciborskiej 28 (budynek Przychodni, II piętro) za pomocą Platformy zakupowej.

Wadium należy wnieść do dnia **15.02.2021r. do godziny 10:00.**

DYREKTOR
Katowickiego Centrum Onkologii

lek. med. Włodzimierz Migacz

 **Śląskie.**

Jednostka ochrony zdrowia Samorządu Województwa Śląskiego.



