Załącznik nr 3 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Macierze

Wymagane jest dostarczenie 2 szt. macierzy w szczególności spełniających poniżej opisane minimalne parametry funkcjonalne:

WYMAGANIA MINIMALNE
- Macierz o wysokości 2U, posiadająca dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji min. 24 dysków. - Macierz musi umożliwiać rozbudowę o moduły: 12 dysków 3,5” o wysokości 2U, 24 dysków 2,5” o wysokości 2U. - Macierz musi posiadać dwa kontrolery w jednej obudowie. - Macierz musi posiadać szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.
Macierz musi być wyposażona w: - 24 dysków 2,5” SSD o pojemności min. 1,8TB każdy, SAS, 12 Gb/s, - Dodatkowy moduł z 12 dyskami 3,5” o pojemności min. 8TB każdy, 12Gb, 7,2k RPM
min. 32 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 64GB).
Każdy kontroler musi być wyposażony w 4 porty FC 16Gb, 2 porty 10Gb. Dopuszcza się współdzielenie portów do zarządzania z portami ISCSI.
Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).
1) Macierz musi obsługiwać wolumeny: - zabezpieczone, które gwarantują odporność na awarię jednocześnie dwóch dysków (RAID 6), - zabezpieczone, które gwarantują odporność na awarię jednego dysku (RAID 5), - standardowe poziomy RAID 0, 10. 2) Macierz dyskowa musi umożliwiać dedykowanie przestrzeni równej pojemności dysku fizycznego jako przestrzeni zapasowej HOT-SPARE lub umożliwiać dedykowanie dowolnego dysku fizycznego jako dysku typu HOT-SPARE. 3) Musi istnieć możliwość definiowania dowolnych dysków typu HOT-SPARE. 4) Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone różnymi poziomami RAID jednocześnie. 5) Macierz musi umożliwiać tworzenie kopii migawkowej w taki sposób, aby dane były zabezpieczone innym poziomem RAID, niż dane źródłowe.
Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych.
Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę

danych z pamięci cache w razie utraty zasilania.
Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade'ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).
Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej Vmware oraz Linux
Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster.
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: MS Windows, Vmware, Linux.
Wykonywanie rozbudowy sprzętowej w trybie online.
Umożliwia rozbudowę do minimum 220 dysków.
Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu.
Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej. Macierz musi posiadać możliwość kompresji lub deduplikacji danych. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie.
Oprogramowanie do zarządzania macierzą przez administratora w ramach pamięci masowej z jednej konsoli administracyjnej.
Stałe monitorowanie macierzy przez zdalne centrum serwisowe.
Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O
Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.
Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków w zależności od stopnia obciążenia macierzy dyskowej. Jeżeli wymagana jest dodatkowa licencja na tą funkcjonalność to powinna być zawarta w cenie
Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie.
Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta.
Możliwość tworzenia i utrzymywania jednocześnie lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora.
Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej.
Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot. Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy.
Kopie migawkowe muszą mieć możliwość prezentacji jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć.
Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na

poziomie poszczególnych wolumenów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie.
Możliwość integracji środowiska Vmware, Veritas InfoScale
Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym bez użycia dodatkowych serwerów lub innych urządzeń. Należy dołączyć licencję, jeśli jest wymagana.
Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem.
Wymagane do replikacji jest użycie protokołu FC
Oferowana macierz dyskowa musi umożliwiać wykonanie w trybie synchronicznym i asynchronicznym zdalnej kopii danych całej powierzchni użytkowej macierzy.
Wymiana dysków może być dokonywana przez Zamawiającego
Szyny do montażu w szafie rack 19''.
Okres gwarancji min 60miesięcy Okres dostępności gwaranta 24x7x365 Gwarantowany czas naprawy 24h

Przełączniki SAN

Wymagane jest dostarczenie 4 szt. przełączników SAN w szczególności spełniających poniżej opisane minimalne parametry funkcjonalne:

WYMAGANIA MINIMALNE
Przełącznik FC musi być wykonany w technologii FC 32 Gb/s i posiadać możliwość pracy portów FC z prędkościami 32, 16, 8 z funkcją autonegocjacji prędkości.
Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla 24 portów FC przełącznika.
Przełącznik musi być dostarczony wraz z minimum 22 modułami SFP FC 16 Gb/s oraz dwoma modułami LW min. 16Gb/s.
Rodzaj obsługiwanych portów: D_Port (ClearLink Diagnostic Port), E_Port, F_Port, M_Port (Mirror Port);
Przełącznik FC musi mieć wysokość maksymalnie 1U i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.
Przełącznik FC musi posiadać nadmiarowe wentylatory N+1
Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
Urządzenie musi umożliwiać połączenie przełączników w jeden „fabric” (funkcjonalność ISL), dostarczyć licencje jeśli wymagane.
Przełącznik FC musi udostępniać usługę Name Server Zoning – tworzenia stref (zon) w oparciu bazę danych

WYMAGANIA MINIMALNE
nazw serwerów.
Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: - Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric - Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP - Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP - Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów - Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, - Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. - Konta użytkowników definiowane w środowisku RADIUS lub LDAP - Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS - Obsługa SNMP v3
Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km.
Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC
Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)
Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP
Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.
Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns.
Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN
Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID.
Możliwość wymiany w trybie „na gorąco": minimum w odniesieniu do modułów portów Fibre Channel (SFP).
Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na

WYMAGANIA MINIMALNE
pojedynczym porcie przełącznika.
Szyny do montażu w szafie rack 19’’.
Okres gwarancji min 60miesięcy Okres dostępności gwaranta 24x7x365 Gwarantowany czas reakcji w tym samym dniu roboczym

Serwer wirtualizacyjny 6 szt.

WYMAGANIA MINIMALNE
Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być wyprodukowana przez producenta serwera
Zainstalowany jeden procesor szesnastordzeniowy min. **3.4GHz** umożliwiający osiągnięcie wyniku **min. 236** w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów. dedykowany do pracy w serwerach dwuprocesorowych
- 768GB RDIMM 2666MT/s, na płycie głównej powinny znajdować się minimum 24 sloty przeznaczone do rozbudowy pamięci.
Memory Rank Sparing, Memory Mirror, ECC
Wbudowane lub dołożone dwuportowa 10GbE SFP+. Kartę dostarczyć wraz z wkładkami 10GBASE SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie. Zainstalowana karta dwuportowa FC 16Gb z modułami
Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowany dedykowany moduł dla hypervisora wirtualizacyjnego, wyposażony w nośniki typu flash o pojemności min. 32GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
- min. 1 port USB 2.0 oraz 2 porty USB 3.0, - 2 porty video (1 na przednim panelu obudowy, drugi na tylnym)
Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440 x 900
Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Redundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera.
Płyta wyposażona w moduł TPM.
Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy.
Zintegrowany z płytą główną serwera, niezalezny od systemu operacyjnego, sprzętowy kontroler zdalnego

zarzadzania z dostępem przynajmniej przez port Ethernet RJ-45 i umożliwiający: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - możliwość zamontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla Ipv6; - SNMP; IPMI2.0, SSH, SNMP; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla dynamic DNS NTP - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
- Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 - Serwer musi posiadać deklaracja CE - Serwer musi posiadać wsparcie dla oferowanego systemu wirtualizacyjnego
- 60 miesięcy wsparcia producenta w trybie pełnego serwisu on-site z gwarantowanym czasem naprawy 24h.

Serwer bazodanowy

WYMAGANIA MINIMALNE
Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być wyprodukowana przez producenta serwera
Zainstalowane dwa procesory ośmiordzeniowe min. **3.6GHz** umożliwiający osiągnięcie wyniku **min. 131** w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów. dedykowany do pracy w serwerach dwuprocesorowych
- 256GB RDIMM 2666MT/s, na płycie głównej powinny znajdować się minimum 24 sloty przeznaczone do rozbudowy pamięci.
Memory Rank Sparing, Memory Mirror, ECC
Wbudowane lub dołożone dwuportowa 10GbE SFP+. Kartę dostarczyć wraz z wkładkami 10GBASE SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z

przełącznikiem w szafie. Zainstalowane dwie karty jednoportowe FC 16Gb z modułami
Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 2 dyski 600GB sas 10K
Zainstalowany kontroler raid z obsługą min RAID 0/1/10
- min. 1 port USB 2.0 oraz 2 porty USB 3.0, - 2 porty video (1 na przednim panelu obudowy, drugi na tylnym)
Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440 x 900
Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Redundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera.
Płyta wyposażona w moduł TPM.
Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy.
Zintegrowany z płytą główną serwera, niezalezny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania z dostępem przynajmniej przez port Ethernet RJ-45 i umożliwiający: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - możliwość zamontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla Ipv6; - SNMP; IPMI2.0, SSH, SNMP; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla dynamic DNS NTP - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
- Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 - Serwer musi posiadać deklaracja CE - Serwer musi posiadać wsparcie dla systemów operacyjnych minimum : Microsoft Windows 2016/2019, RedHat Enterprise Linux 7 oraz 8
- 60 miesięcy wsparcia producenta w trybie pełnego serwisu on-site z gwarantowanym czasem naprawy 24h.

Serwerowy system operacyjny

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:
Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.
Licencje muszą zostać dostarczone dla każdego z serwerów wirtualizacji na ilość rdzeni zgodną z dostarczanym procesorem .

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:

9.1. pozwalają na zmianę rozmiaru w czasie pracy systemu,

9.2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

9.3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

9.4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

15.1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

15.2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18. Mechanizmy logowania w oparciu o:

18.1. Login i hasło,

18.2. Karty z certyfikatami (smartcard),

18.3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

25.1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

25.2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

25.2.1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

25.2.2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

25.2.3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

25.2.4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

25.3. Zdalna dystrybucja oprogramowania na stacje robocze.

25.4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

25.5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

25.5.1. Dystrybucję certyfikatów poprzez http

25.5.2. Konsolidację CA dla wielu lasów domeny,

25.5.3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

25.5.4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

25.6. Szyfrowanie plików i folderów.

25.7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

25.8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

25.9. Serwis udostępniania stron WWW.

25.10. Wsparcie dla protokołu IP w wersji 6 (IPv6),

25.11. Wsparcie dla algorytmów Suite B (RFC 4869),

25.12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

25.13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

25.13.1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

25.13.2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

25.13.3. Obsługi 4-KB sektorów dysków

25.13.4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

25.13.5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

25.13.6. 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.

Licencje dostępowe do serwerowego systemu operacyjnego

W ramach zamówienia Wykonawca zobowiązany jest dostarczyć licencje dostępowe serwera zgodnie

z poniższymi wymaganiami:

Wymagane jest dostarczenie serwerowych licencji dostępowych typu CAL dla dostarczonego Serwerowego systemu operacyjnego, opisanego szczegółowo w SIWZ w następujących ilościach :

Licencje dostępowe na urządzenie 1000szt.
Licencje uprawniające do dostępu zdalnego na urządzenie 1000szt.

Oprogramowanie systemowe storage

Minimalne wymagania na oprogramowanie systemowe storage:

Rozbudowa posiadanego przez zamawiającego oprogramowania Veritas Infocale Enterprise o dodatkowe

licencje na 4core ze wsparciem producenta do 30.09.2023 oraz uzupełnienie wsparcia do dnia 30.09.2023

dla posiadanych przez Zamawiającego licencji. Zamawiający aktualnie posiada 28szt. Veritas InfoSCALE

Enterprise gov.

Oprogramowanie wirtualizacyjne

Minimalne wymagania na oprogramowanie do wirtualizacji serwerów:

WYMAGANIA MINIMALNE
Wykonawca zobowiązany jest do dostarczenia kompletu licencji oprogramowania do wirtualizacji instalowanego na dostarczanych serwerach wirtualizacyjnych, obejmujących łącznie 6 procesorów fizycznych oraz licencji dla potrzeb centralnej konsoli graficznej dla 6 hostów do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Licencje powinny być bezterminowe oraz dostarczone z 5 letnim wsparciem
Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.
Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 300 MB pamięci operacyjnej RAM serwera fizycznego.
Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym.
Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.
Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
Rozwiązanie musi wspierać następujące systemy operacyjne na maszynie wirtualnej: Windows Server 2008, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, SLES 12, SLES 11, SLES 10, RHEL 7, RHEL 6, RHEL 5, RHEL 4, Solaris wersja 11 dla platformy x86, Solaris wersja 10 dla platformy x86
Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową, minimum IE, Firefox, Chrome w najnowszych wersjach.
Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji, bez konieczności instalowania agenta oprogramowania na maszynie wirtualnej.
Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.

Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, LDAP.
Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o łącznej liczbie rdzeni nie przekraczającej 32 rdzeni per procesor.
Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
Rozwiązanie musi gwarantować współczynnik RPO na poziomie przynajmniej 15 minut
Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi wirtualnymi przełącznikami sieciowymi
Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej lub partycjonowania sieci.
Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi, klastrami, centrami przetwarzania danych bez przerywania pracy usług.

Oprogramowanie do kopii zapasowych

Minimalne wymagania dla oprogramowanie do kopii zapasowych:

Rozbudowa posiadanego przez zamawiającego oprogramowania Veritas Netbackup o dodatkowe licencje na 2T complete gov wraz ze wsparciem producenta do 30.09.2023 oraz uzupełnienie wsparcia do do dnia 30.09.2023 do posiadanych przez Zamawiającego licencji Veritas NetBackup 1T Complete gov szt.3

Terminal

W ramach rozbudowy środowiska terminalowego dostawa 150 terminali SunRay bez klawatury lub równoważnych współpracujących z posiadaną przez Zamawiającego infrastrukturą SunRay.

Zakres usługi wdrożeniowej

1. Dostawa i instalacja
2. Migracja obecnego środowiska vmware
3. Rekonfiguracja i migracja przestrzeni macierzowych
4. Upgrade środowiska Windows (Active Directory + Profile Mobilne + Klaster Windows)
5. Przebudowa i migracja rozległej sieci SAN
6. Rekonfiguracja i migracja środowiska klastrowego Veritas z bazami danych Oracle aplikacji medycznych.
7. Rekonfiguracja środowiska terminalowego SunRay
8. Rekonfiguracja przestrzeni pod system Agfa
9. Testy i dokumentacja

Wszelkie prace wykonywane będą na środowisku produkcyjnym szpitala z zachowaniem odpowiednich procedur bezpieczeństwa przez wykonawcę .

…….. **……...**

data **podpis Wykonawcy**