Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ) - MODERNIZACJA INFRASTRUKTURY

(aktualizacja z dnia 10.05.2018 r.)

SERWEROWO-MACIERZOWEJ I SIECIOWEJ

Szafa serwerowa typu RACK z akcesoriami - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Minimum 42U, maximum 43U o wymiarach 600mm szerokości x co najmniej 1070 mm, maximum 1270 Głębokości z możliwością instalacji modułów dystrybucji zasilania Zero U
Wentylacja	Panel wentylacyjny umieszczony w dachu obudowy
Moduły dystrybucji zasilania	Zainstalowane dwa moduły dystrybucji zasilania Zero U, 16A, 230V, z gniazdami C13 – 20 szt., C19 – 4 szt, z zasilaniem wtyczką 16A C20
Organizatory kabli	Zainstalowane dwa pionowe organizatory kabli
Warunki gwarancji dla obudowy	Co najmniej trzy lata gwarancji
Instalacja	Zamawiający wymaga wniesienia i instalacji szafy serwerowej w pomieszczeniu wyznaczonym przez Zamawiającego. Zamawiający wymaga instalacji modułów dystrybucji zasilania w szafie wraz z odpowiednim ułożeniem kabli zasilających i podłączeniem ich do zasilaczy awaryjnych UPS

Zasilacz awaryjny – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Moc rzeczywista	3500 Wat
Architektura UPSa	on-line
Liczba i rodzaj gniazdek z utrzymaniem zasilania (dopuszcza się stosowanie zewnętrznych listew/rozgałęźników)	8 x IEC320 C13
Liczba, typ gniazd wyj. z ochroną antyprzepięciową	2 x IEC320 C19
Typ gniazda wejściowego	4 x IEC Jumpers
Czas podtrzymania dla obciążenia 100%	8 min
Czas podtrzymania przy obciążeniu 50%	16 min
Zakres napięcia wejściowego w trybie podstawowym	220-240 V
Zimny start	Tak
Porty komunikacji	RJ-45 10/100 Base-T, RJ-45 serial,
Diody sygnalizacyjne	• konieczna wymiana baterii
	• praca z baterii
	• praca z sieci zasilającej
	• przeciążenie UPSa
Alarmy dźwiękowe	• praca z baterii
	• przeciążenie UPSa
	• znaczne wyczerpanie baterii
Typ obudowy	Rack
Wyposażenie standardowe	• Kabel RJ-45
	• kabel zasilający 1.8m IEC320 C13/C14 - 2 szt.
	• oprogramowanie na CD
	• Instrukcja obsługi
Dołączone oprogramowanie	umożliwiające zdalne zatrzymanie serwerów w przypadku utraty zasilania
Szerokość	Max 610 mm
Wysokość	Max 350 mm
Głębokość	Max 1000 mm
Masa netto	Max 56 kg

Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24 godziny na dobę przez 7 dni w tygodniu przez 365 dni w roku poprzez e-mail lub linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Sprzęt ma być serwisowany bezpośrednio przez serwis producenta lub firmę serwisującą posiadającą ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje/certyfikację producenta zasilacza – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Instalacja	Zamawiający wymaga instalacji zasilaczy awaryjnych w nowo zakupionej szafie RACK. Zamawiający wymaga podłączenia zasilaczy do istniejącej tablicy rozdzielczej i przygotowania do współpracy z istniejącym agregatem prądotwórczym. Kable OMY o przekroju min.6mm2 do podłączenia zasilaczy awaryjnych dostarcza Wykonawca. Wykonanie instalacji przyłączeniowej UPS musi odbyć się przez osoby posiadające ważne uprawnienia SEP do eksploatacji 1kV.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim

Macierz dyskowa 2 szt.

Komponent	Minimalne wymagania
Macierz	Macierz o wysokości nie większej niż 3U, posiadająca co najmniej dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji przynajmniej 30 dysków. Macierz musi umożliwiać rozbudowę o co najmniej moduły: 12 dysków 3,5” o wysokości nie większej niż 2U, 24 dysków 2,5” o wysokości nie większej niż 2U, 60 dysków 3,5” o wysokości nie większej niż 4U. Macierz musi obsługiwać dyski o pojemności min. 15TB Macierz musi obsługiwać dyski do łącznej ilości minimum 220 dysków SAS/NLSAS lub SSD.
Wymagane dyski	Macierz musi być wyposażona w co najmniej: 7 dysków 2,5” SSD o pojemności 960GB, SAS, 12Gb/s Oraz przynajmniej 2 dodatkowe moduły, gdzie w każdym co najmniej: 12 dysków 3,5” 4TB NL-SAS, 12Gb, 7.2k. Całość rozwiązania powinna zajmować łącznie nie więcej niż 7U.
Pamięć podręczna (Cache)	Pamięć podręczna (cache) – co najmniej 64 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie co najmniej 128GB). Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash.
Interfejsy zewnętrzne	Każdy kontroler musi być wyposażony w 2 porty FC 16Gb, 4 porty SFP+, 1 port zarządzający 1GbE Base-T.
Dostępność	Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).
	Możliwość łączenia w macierzy różnych poziomów RAID: możliwość zastosowania RAID10 możliwość zastosowania RAID 10DM, możliwość zastosowania RAID5, możliwość zastosowania RAID6 możliwość zastosowania RAID0 możliwość zastosowania RAID1
	Co najmniej 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).
	Możliwość zdefiniowania min. 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa.
	Możliwość obsługi wirtualnych portów (NPIV) w taki sposób, aby awaria fizycznego portu nie powodowała konieczności przełączania ścieżek poprzez oprogramowanie do multipathing
Wspierane systemy operacyjne	Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej AIX, HP-UX, MS Windows, VMware oraz Linux, APPLE IOS

	Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster Server, HACMP, HP Serviceguard.
	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: AIX, HP-UX, MS Windows, Vmware, Linux.
	Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning.
Skalowalność	Wykonywanie rozbudowy sprzętowej w trybie online.
	Umożliwia rozbudowę do minimum 220 dysków 2,5”.
	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.
Zarządzanie	Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).
	Stałe monitorowanie macierzy przez zdalne centrum serwisowe.
	Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów. Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych.
	Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej do co najmniej 500TB.
	Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.
Możliwość migracji danych w obrębie macierzy	Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków oraz rożnymi poziomami RAID w zależności od stopnia obciążenia macierzy dyskowej. Dane często używane macierz powinny automatycznie przemieszczać na dyski o największej prędkości obrotowej, dane rzadko używane na dyski o prędkości obrotowej 7200 rpm. Dodatkowo funkcjonalność ta musi wspierać dyski SSD zoptymalizowane przez producenta dysków do zapisu lub do odczytu.
	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 cenie oferty.
	Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Musi również umożliwiać udostępnienie tego wolumenu logicznego LUN po protokole FC

Lokalna replikacja danych	Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta.
	Możliwość tworzenia i utrzymywania jednocześnie minimum ośmiu 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. Zamawiający wymaga dostarczenia licencji na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy.
	Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write)
	Kopie migawkowe muszą mieć możliwość prezentacji, jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć.
Redukcja danych	Macierz powinna zapewniać metody redukcji ilości danych blokowych za pomocą kompresji. Kompresja powinna odbywać się po fakcie zapisu na urządzenia dyskowe wewnątrz macierzy (dane spoczynkowe).
Kontrola przepływu danych - QoS	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.
Współpraca z aplikacjami	Możliwość integracji środowiska VMware, Microsoft SQL z mechanizmem lokalnej replikacji danych.
Zdalna replikacja danych (Zamawiający wymaga dostarczenia licencji w cenie oferty)	Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym i asynchronicznym interwałowym 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.
Importowanie danych	Macierz musi posiadać funkcjonalność onlinowego importu danych z macierzy innego producenta z jednoczesną konwersją wolumenu logicznego LUN do trybu „Thin Provision”
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24 godziny na dobę przez 7 dni w tygodniu przez 365 dni w roku poprzez e-mail lub linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Sprzęt ma być serwisowany bezpośrednio przez serwis producenta lub firmę serwisującą posiadającą ISO 9001:2000 na świadczenie usług serwisowych

	oraz posiadać autoryzacje/certyfikację producenta macierzy – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Wymiana dysków	Wymiana dysków może być dokonywana przez Zamawiającego. W przypadku wymiany dysku na nowy, stary dysk zostaje u Zamawiającego.
Wdrożenie	Zamawiający wymaga wdrożenia macierzy w zakresie: - instalacja macierzy dyskowej - konfiguracja tieringu dla dysków - konfiguracja zoningu dla portów FC macierzy w trybie wirtualnym (tzn. każdy port kontrolera jest w trybie active) - podłączenie 4 nowo zakupionych serwerów do macierzy podstawowej i zapasowej w technologii Fibre Channel i iSCSI - podłączenie 4 istniejących serwerów do macierzy podstawowej i zapasowej w technologii iSCSI (podłączenie nowo zakupionej macierzy musi odbyć się w trybie on-line – tzn. nie może spowodować przestoju w pracy Zamawiającego) - konfigurację wolumenów dla klastra wirtualizacji dla starych i nowych serwerów - stworzenie polityk QoS umożliwiających replikację macierzy - replikację wolumenów pomiędzy macierzami w technologii umożliwiającej przełączenia wolumenów pomiędzy aktywną a replikowaną macierzą w locie (tzn. macierz podstawowa dla dowolnego wolumenu może być macierzą replikującą, przełączenie musi odbywać się on-line bez potrzeby wyłączania serwerów w celu zmiany repliki) - migrację danych z istniejącej podstawowej macierzy iSCSI MD3200i na nowo zakupione macierze - rekonfigurację istniejącej macierzy jako macierz do tworzenia kopii zapasowych Wszelkie prace migracyjne wymagające wyłączenia usług Zamawiającego muszą być zaplanowane po godzinach pracy urzędu Zamawiającego. Instalacja macierzy musi zostać tak zaplanowana aby jedną z nich można było bez problemowo przenieść z całą szafa do innej lokalizacji na terenie miasta Gdyni. W szafie tej musi znaleźć się również serwer kopi zapasowej DPM ze storage Iomega PX6-300d aktualnie wykorzystywany przez Zamawiającego. Oprogramowanie DPM należy podnieść do najnowszej dostępnej wersji.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Wyposażenie dodatkowe do oddziału z replikacją	Patchcord światłowodowy Single Mode Duplex 9/125 SC-PC/LC-PC 10m – 8 szt. Patchcord UTP LSOH RJ45 3m – 12 szt. Patchcord UTP LSOH RJ45 1m – 8 szt. Wkładka światłowodowa 10GE LR (DWDM) – 4 szt. (tu zależy ile będzie tych ciemnych włókien)

Obudowa serwerowa dla serwerów blade – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Maksimum 10U do instalacji w standardowej szafie serwerowej Rack 19” Obudowa musi umożliwiać instalację w niej aktualnie wykorzystywanych przez Zamawiającego serwerów tj. Serwerów Dell PowerEdge M610.
Ilość serwerów	Obudowa powinna umożliwiać instalację minimum 16 wymaganych poniżej serwerów dwuprocesorowych bez konieczności rozbudowy o dodatkowe komponenty. Zainstalowane 4 Serwery Typ 1
Konwergentne moduły rozszerzeń 10Gb	Zainstalowane moduły 10Gb: a) 2 moduły zarządzalnych przełączników warstwy 3, w każdym zintegrowane 32 porty 10Gb Ethernet (32 wewnętrznych i 4 zewnętrzne SFP+). Dostępna rozbudowa poprzez wymienne wewnętrzne moduły: - 4-portowy moduł 10 GbE SFP+ (z obsługą połączeń 1/10 GbE) - 4-portowy moduł Fibre Channel - 4-portowy moduł 10 GbE Base-T (z obsługą połączeń 1/10 GbE) - 2-portowy moduł 40 GbE QSFP+ (z obsługą połączeń 40 GbE) b) Prędkość przełączania: całkowita przepustowość min. 1 Tb/s (dwukierunkowa) c) Prędkość przekazywania: min 900 milionów pakietów na sekundę d) Obsługa 16000 adresów MAC
Moduły rozszerzeń FC16	Zainstalowane 2 moduły przełączników Hot-Plug I/O FC16 obsługujące wewnętrzne karty FC w układzie wszystkie pierwsze interfejsy z każdego serwera przyłączone do pierwszego modułu, drugie interfejsy do drugiego modułu. Aktywne minimum 16 portów wewnętrznych i 4 zewnętrzne. Możliwość rozbudowy 8 zewnętrznych portów na każdy moduł
Dodatkowe moduły rozszerzeń I/O	Przynajmniej 2 dodatkowe zatoki umożliwiające instalację następujących modułów Hot-Plug: - switchy Gigabit Ethernet - switchy 10G - switchy FC 8Gb - switchy InfiniBand
Zarządzanie	Zintegrowany z obudową moduł switcha KVM umożliwiający przyłączenie lokalne (analogowe) monitora, klawiatury i myszy. System powinien mieć zainstalowane w obudowie blade dwie karty zdalnego zarządzania (Hot-Plug) pracujące w redundancji. Wymiana jednej z nich nie powinna powodować przerw w dostępie do drugiej. System zarządzania powinien umożliwiać: dostęp przez sieć LAN 10/100 Mb (osobne wyjście, własne IP sieci zarządzającej), zdalne włączanie i wyłączanie serwerów blade, podgląd logów sprzętowych serwera i karty, a także zarządzanie poszczególnymi serwerami (przejęcie ich konsoli w trybie graficznym i tekstowym – także w sesji BIOS, podłączenie wirtualnych napędów). Możliwość zarządzania jednocześnie wszystkimi serwerami blade, podgląd poboru energii całej obudowy i poszczególnych serwerów w trybie online. Wymagana możliwość zdalnego update i konfiguracji BIOS oraz detekcji przedawaryjnej. System musi umożliwiać wysyłanie przez e-mail komunikatów o błędach do administratorów. Karty zarządzające powinny mieć możliwość przechowywania wszystkich MAC adresów kart sieciowych

	serwerów oraz adresów WWN niezależnie od zainstalowanych przełączników. Obudowa wyposażona w wyświetlacz LCD umożliwiający diagnostykę.
Zasilanie	Obudowa musi być wyposażona w min. 6 zasilaczy Hot-Plug pracujących w redundancji: możliwe do zdefiniowania tryby pracy N+N oraz N+1
Wentylacja	System musi zapewniać sprawną wentylację wszystkich serwerów zamontowanych w obudowie nie dopuszczając do ich przegrzania. Producent musi zagwarantować, że dla maksymalnej liczby serwerów w szafie rack wentylatory w obudowach zapewnią wydajne chłodzenie dla wszystkich urządzeń w maksymalnych konfiguracjach przy założeniu dostarczenia przed szafę powietrza o tmax 25 stopni C. Wentylatory muszą być redundantne typu Hot-Plug.
Warunki gwarancji dla obudowy	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24 godziny na dobę przez 7 dni w tygodniu przez 365 dni w roku poprzez e-mail lub linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Sprzęt ma być serwisowany bezpośrednio przez serwis producenta lub firmę serwisującą posiadającą ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje/certyfikację producenta obudowy – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Wdrożenie	Zamawiający wymaga wdrożenia obudowy blade w następującym zakresie: - instalacja obudowy w aktualnie wykorzystywanej szafie. Aktualnie wykorzystywana klatka Blade musi zostać przeniesiona do nowej szafy. - podłączenie zasilania obudowy do dwóch PDU zasilanych z osobnych zasilaczy awaryjnych UPS - konfiguracja obudowy blade w następującym zakresie: uruchomienie redundantnych kontrolerów CMC, nadanie adresacji Out Of Band dla kart IO, serwerów zainstalowanych w Chassis, uruchomienie kart zarządzających serwerów Blade, skonfigurowanie SNMP dla systemów monitoringu
Konfiguracja konwergentnych modułów 10Gb	Zainstalowanie kart 10GE z modułami SFP+ będących w posiadaniu Zamawiającego. Rekonfiguracja istniejących przełączników w starej obudowie Blade w zakresie VLT, Vlan, routingu, list dostępowych, adresacji, QoS, obsługi ruchu konwergentnego (DATA,iSCSI) oraz obsługi autoryzacji 802.1X Konfiguracja przełączników w zakresie Vlan, routingu, list dostępowych, adresacji QoS, obsługi ruchu konwergentnego (DATA,iSCSI) oraz obsługi autoryzacji 802.1X

Konfiguracja modułów rozszerzeń FC16	Konfiguracja zoningu dla serwerów i urządzeń sieci SAN na przełączniku FC. Konfiguracja portów przełącznika do współpracy z nowo zakupionymi macierzami w zakresie zoningu, virtual ports, aliasów oraz konfiguracji QoS do replikacji.

Przełącznik sieciowy warstwy 3 - typ A - 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Producent	Nazwa producenta:
Identyfikacja	Typ produktu, model:
Ilość portów	Co najmniej 48 x 10GbE SFP+, 6 x QSFP+
Wymiar	19 cali – do montażu w szafie rakowej, wysokość max 1 U
Inne	Liczba adresów MAC: 160K Ilość tras IPv4: 128K Ilość tras IPv6: 64K opóźnienie poniżej 600ns Prędkość przełączania 1.44 Tbps (full-duplex) L2 Vlan: 4K Kolejki QoS: min 8 Wspacie dla VLAN, wsparcie dla GVRP Obsługa routingu co najmniej : statyczny, RIP, OSPF również w wersji 3,BGP Obsługa Virtual Redundant Routing Protocol (VRRP) Obsługa LLDP-MED Obsługa IPv6 Obsługa PVST Obsługa DCB MTU co najmneij 12000
Obsługiwane standardy	VLAN – IEEE 802.1Q, 802.3ac, 802.1Qbb, 802.1Qaz QoS – IEEE 802.1p Link Aggregation – IEEE 802.3ad Edge Authentication – IEEE 802.1x Rapid Spanning Tree – IEEE 802.1w Multiple Spanning Trees – IEEE 802.1s 10 Gigabit Ethernet (10GBASE-X) - IEEE 802.3ae 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4) -IEEE802.3ba on optical ports Industry-standard MIB support
Zarządzanie, zabezpieczenia	Połączenie szyfrowane: autentykacja dostępu w oparciu o Radius oraz na podstawie MAC adresu, listy dostępu; RMON, CLI, SNMP v3
Kable i moduły	Kabel Direct Attach QSFP+ - QSFP+ 40GE 3m – 4 szt. Kabel Direct Attach QSFP+ - QSFP+ 40GE 15m – 4 szt. Kabel Direct Attach SFP+ - SFP+ 10GE 0,5m – 4 szt. Kabel Direct Attach SFP+ - SFP+ 10GE 3m – 8 szt. Kabel Direct Attach SFP+ - SFP+ 10GE 15m – 8 szt.
Warunki gwarancji	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24 godziny na dobę przez 7 dni w tygodniu przez 365 dni w

	roku poprzez e-mail lub linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta przełącznika – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisie.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Wdrożenie	Zamawiający wymaga konfiguracji przełączników jako warstwy CORE. Obecnie istniejące przełączniki MXL zainstalowane w obudowie Blade pełnią rolę warstwy core dla warstwy dostępowej oraz serwerów. Zamawiający wymaga przeniesienia obecnej konfiguracji na nowo zakupione przełączniki, w szczególności: • konfiguracja VLAN dostępowych • konfiguracja DHCP • konfiguracja routingu dynamicznego (z przygotowaniem redystrybucji tras OSPF do zamkniętego protokołu CISCO EIGRP) • konfiguracja routingu statycznego • podłączenie do serwerów uwierzytelnienia TACACS+ • konfiguracji SNMP • instalacją i konfiguracją oprogramowania do monitorowania przełączników minimalnie dostępne statystyki w interwałach 5min, 1h, dziennym, tygodniowym, miesięcznym: o obciążenie procesora o statystyki ruchu wszystkich portów sieciowych, w tym statystki ruchu dla każdego z VLAN • konfiguracją QoS • konfiguracją Policy Base Routing – ruch z/do VPN ma odbywać się do routerów obsługujących DMVPN, ruch z/do internetu ma odbywać się przez urządzenia obsługujące internet Konfiguracja Spanning-Tree, przełączniki core mają pełnić rolę Root dla całej topologii sieci w centrali. Konfiguracja protokołów redundancji przełączników (restart, uaktualnienie oprogramowania na jednym z przełączników nie może powodować przerw w działaniu całej sieci) oraz protokołów redundancji łącza podstawowego VRRP. Zamawiający wymaga połączenia przełączników core z istniejącym stosem przełączników CISCO 3750X i rekonfiguracji połączeń do routerów/urządzeń dostępowych do internetu jak i redystrybucji dynamicznego routingu pomiędzy protokołami OSPF oraz EIGRP. Rekonfiguracja protokołów dynamicznego routingu nie może spowodować przerwy w działaniu sieci tj. wszystkie oddziały podłączone do centrali nie mogą utracić połączeń do serwerów.

	Przełączenie i rekonfiguracja przełączników dostępowych CISCO 2960X do przełącznika CORE, obecnie przełączniki 2960X są wpięte w VLT przełączników Blade MXL. Ewentualne przestoje wynikające z przepięcia przełączników dostępowych 2960X należy zaplanować poza godzinami pracy urzędu Zamawiającego.

Przełącznik sieciowy typ B – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Ilość portów	Minimum 24 portów 10/100/1000 Minimum 2 dodatkowe porty 10 Gigabit Ethernet SFP+. Porty muszą umożliwiać ich obsadzanie wkładkami: SPF+ 10 Gigabit Ethernet – minimum 10GBase-SR, LR oraz SPF Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX/LH zależnie od potrzeb Zamawiającego.
Wymiar	19 cali – do montażu w szafie rakowej, wysokość max 1 U
Łączenie w stos	Funkcjonalność łączenia w stosy zarządzany jak pojedyncze urządzenie z zachowaniem następującej parametrów: do min. 8 jednostek w stosie, magistrala stackująca o przepustowości co najmniej 40Gb/s możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel) UWAGA: jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów, kabli itp. ich dostarczenie w ramach tego postępowania JEST WYMAGANE. Zamawiający dopuszcza stackowanie po portach uplink pod warunkiem, że będą to porty dodatkowe w stosunku do wymaganych i pozwolą na uzyskanie pełnej funkcjonalności opisanej wyżej (w tym wymaganą przepustowość magistrali stackującej)
Pamięć	Co najmniej 512MB pamięci DRAM oraz co najmniej 128MB pamięci Flash
Wielkość tablicy adresów MAC	Co najmniej 32 000
Ilość obsługiwanych sieci VLAN	Co najmniej 2 000
Wydajność	Przepustowość zapewniająca wydajność Line-rate co najmniej 160 Gbps Przełączanie dla pakietów 64-bajtowych: min. 128 Mpps.
Obsługa ramek Jumbo	O wielkości co najmniej 9216 bajtów
Funkcjonalność urządzenia	Obsługa VLAN IEEE 802.1Q , Obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad), Obsługa Spanning Tree (IEEE 802.1d/w), Obsługa QoS (co najmniej 8 kolejek per port), Voice VLAN, LLDP-MED lub CDP Obsługa IEEE 802.1x, Obsługa Energy Efficient Ethernet (IEEE 802.3az), Obsługa mechanizmów bezpieczeństwa L2 – DHCP snooping, IP Source Guard, Dynamic ARP inspection, RA Guard, Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) - zarówno dla IPv4 jak i IPv6, Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne),

	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie co najmniej następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
Zarządzanie, zabezpieczenia	Co najmniej poprzez protokoły: SNMP, SSH, HTPP/HTTPS z wykorzystaniem IPv4 i IPv6
Kable	Wymagane jest by przełącznik wyposażony był w kable do połączenia w stos
Warunki gwarancji	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24 godziny na dobę przez 7 dni w tygodniu przez 365 dni w roku poprzez e-mail lub linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Sprzęt ma być serwisowany bezpośrednio przez serwis producenta lub firmę serwisującą posiadającą ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje/certyfikację producenta przełącznika – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Wdrożenie	Instalacja przełączników w szafie RACK Konfiguracja przełączników do współpracy z serwerem backupu oraz protokołami iSCSI Rekonfiguracja istniejących macierzy dyskowych MD3200i oraz IOMega px6-300d do współpracy z przełącznikiem. Obecnie ruch iSCSI jest obsługiwany przez przełączniki M6220 zainstalowane w obudowie Blade oraz przez przełączniki dystrybucyjne CISCO 3750X. Zamawiający wymaga przeniesienia wszystkich urządzeń iSCSI biorących udział w procesie backupu do nowo zakupionych przełączników.

Serwer typu blade A – 4 szt.

Parametr	Charakterystyka (Minimalne wymagania)
Obudowa	Typu blade, umożliwiająca zainstalowanie min. 16 sztuk zaoferowanych serwerów w dostarczanej wraz z serwerami obudowie Blade. (Jeżeli oferowana obudowa nie posiada takiej możliwości, należy dostarczyć taką ilość obudów Blade wraz z wymaganymi przełącznikami, aby możliwa była instalacja łącznie minimum 16 sztuk serwerów.) Obudowa serwera musi mieć możliwość instalacji w aktualnie wykorzystywanej przez Zamawiającego klatce Blade M1000e.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów cztero-, sześćio-, ośmio-, dziesięcio-, dwunasto-, czternasto-, szesnasto-, osiemnasto-, dwudziesto-, dwudziesto-dwu, dwudziesto-cztero oraz dwudziesto-ośmio-rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Dwa procesory ośmio-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 17500 punktów w teście PassMark CPU Benchmark z dostępnym na stronie cpubenchmark.net. Wynik testu dla oferowanego procesora musi być opublikowany na stronie https://www.cpubenchmark.net/high_end_cpus.html (obowiązują wyniki testu wydajności CPUBenchmark ® aktualnego na dzień 12.04.2018 r. – stanowiące załącznik nr 1 do niniejszego OPZ)
Pamięć RAM	Płyta musi obsługiwać do 1TB pamięci RAM RDIMM/LRDIMM o częstotliwości pracy do 2667 MT/s, na płycie głównej musi znajdować się co najmniej 16 slotów na pamięci. Musi posiadać zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling, SBEC. Zainstalowane min. 384GB RAM w nie więcej niż 6 kościach
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 1x USB 2.0 i 1x USB 3.0 na przednim panelu obudowy obsługujące bootowanie z napędów: dyskietek, CD/DVD, klucza USB oraz 1x USB 3.0 wewnątrz obudowy. Zamawiający nie dopuszcza realizacji poprzez zastosowanie przejściówek, adapterów oraz modułów lub kabli rozszerzających.
Interfejsy LAN	Min. 4 interfejsy 10GbE
Interfesy SAN	Min. 2 interfejsy FC 16 GB/s
Wewnętrzna pamięć masowa	Możliwość instalacji 2 dysków twardych SATA, SAS, SSD, NVMe SSD. Zainstalowane : 2 x 480 GB SSD RI
	Możliwość instalacji wewnętrznych modułów dedykowanych dla hypervisora wirtualizacyjnego, wyposażonego w dwa jednakowe nośniki typu flash o pojemności min. 8GB z możliwością

	skonfigurowania zabezpieczenia typu "mirror" pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM 1.2 lub 2.0
Karta zarządzająca	Niezależna od zainstalowanego na serwerze systemu operacyjnego umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6 - wsparcie dla: SNMP; IPMI2.0, VLAN tagging, Telnet, SSH - 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 - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, - możliwość zablokowania rekonfiguracji serwera i aktualizacji firmware przez jednego administratora w przypadku gdy jest wielu administratorów, - automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) zapisanych na dedykowanej pamięci flash wbudowanej na karcie zarządzającej
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24 godziny na dobę przez 7 dni w tygodniu przez 365 dni w roku poprzez e-mail lub linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Sprzęt ma być serwisowany bezpośrednio przez serwis producenta lub firmę serwisującą posiadającą ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje/certyfikację producenta serwera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy

	serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Zgodność z wirtualizatorami Citrix, Vmware vSphere, Microsoft Hyper-V. Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Windows Server 2012, Windows Server 2012R2, Windows Server 2016.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Wdrożenie	Zamawiający wymaga uruchomienia serwerów i instalacji nowo zakupionego oprogramowania do pracy na serwerach. Zamawiający wymaga stworzenie klastra typu Failover na nowo zakupionych serwerach dla potrzeb wirtualizacji zasobów serwerowych. Zamawiający wymaga migracji wszystkich maszyn wirtualnych z istniejącego klastra Windows Server 2012 R2 na nowo zakupione serwery. Zamawiający wymaga podniesienia wersji oprogramowania na wirtualnych Kontrolerach domeny(Zamawiający dopuszcza wystawienie nowych wirtualnych co najmniej 2 kontrolerów domeny w najnowszej dostępnej wersji), do najnowszej obowiązującej wersji w trakcie wdrożenia – jeżeli będzie to wymagane Zamawiający dostarczy odpowiednie licencje. Zamawiający wymaga podniesienia wersji starego klastra wirtualizacji do najnowszej obowiązującej wersji oraz stworzenie repliki wybranych maszyn wirtualnych na istniejącym systemie. Jeżeli prace wdrożeniowe wymagają wyłączenia któregokolwiek z systemów i przerwania pracy Zamawiającego to wymagane jest zaplanowanie ich poza godzinami pracy urzędu Zamawiającego. Stworzenie wirtualnej instancji serwera w najnowszej możliwej wersji pod drugi serwer kopii zapasowej DPM, którego dane znajdować będą się na obecnie wykorzystywanych urządzeniach Iomega PX6-300d oraz Macierzy Dell MD3200i

Oprogramowanie serwerowe A - Zintegrowany pakiet oprogramowania do tworzenia i zarządzania środowiskami wirtualnymi z oprogramowaniem systemowym wraz z wdrożeniem – 4 serwery z pełnym pokryciem rdzeni fizycznych.

Parametr	Charakterystyka (wymagania minimalne)
Oprogramowanie	**Zintegrowany pakiet oprogramowania do tworzenia i zarządzania środowiskami wirtualnymi** Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na fizyczne rdzenie procesora serwera zarządzanego. Licencja na fizyczne rdzenie procesora serwera musi uprawniać do zarządzania nielimitowaną ilością środowisk systemu operacyjnego na tym serwerze. Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach: • System zarządzania infrastrukturą i oprogramowaniem • System zarządzania komponentami • System zarządzania środowiskami wirtualnym • System tworzenia kopii zapasowych • System automatyzacji zarządzania środowisk IT • System zarządzania incydentami i problemami • Ochrona antymalware **System zarządzania infrastrukturą i oprogramowaniem** System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. 1. Inwentaryzacja i zarządzanie zasobami: a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania b. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu c. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów

	wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp…) d. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera 2. Użytkowane oprogramowanie – pomiar wykorzystania a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego. 3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych. 4. Definiowanie i sprawdzanie standardu serwera: a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej, b. Reguły powinny sprawdzać następujące elementy systemy komputerowego: − stan usługi (Windows Service) − obecność poprawek (Hotfix) − WMI − rejestr systemowy − system plików − Active Directory − SQL (query) − Metabase 5. Raportowanie, prezentacja danych: a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub

	b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services c. System powinien posiadać predefiniowane raport w następujących kategoriach: − Sprzęt (inwentaryzacja) − Oprogramowanie (inwentaryzacja) − Oprogramowanie (wykorzystanie) − Oprogramowanie (aktualizacje, w tym system operacyjny) d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu 6. Analiza działania systemu, logi, komponenty a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym. **System zarządzania komponentami** System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania: 1. Architektura a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji. b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług. c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych. d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na

	klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny. e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych. f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany. g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN). h. Wsparcie dla protokołu IPv6. i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta. 2. Audyt zdarzeń bezpieczeństwa System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować: a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących). b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji. c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów. 3. Konfiguracja i monitorowanie System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym: a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:

	- rejestru - WMI - OLEDB - LDAP - skrypty (uruchamiane w celu wykrycia atrybutów obiektu), W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi. b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp… c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla: - Windows Server 2003/2008/2008R2 - Active Directory 2003/2008 - Exchange 2003/2007/2010 - Microsoft SharePoint 2003/2007/2010 - Microsoft SharePoint Services 3.0 - Microsoft SharePoint Foundation 2010 - SQL 2005/2008/2008R2 (x86/x64/ia64) - Windows Client OS (XP/Vista/7) - Information Worker (Office, IExplorer, Outlook, itp…) - IIS 6.0/7.0/7.5 - HP-UX 11i v2/v3 - Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86) - Red Hat Enterprise Linux 4/5/6 (x86/x64) Server - Novell SUSE Linux Enterprise Server 9/10SP1/11 - IBM AIX v5.3 i v6.1/v7.1 (POWER) d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego. e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji: - interfejsy sieciowe - porty - sieci wirtualne (VLAN)

	- grupy Hot Standby Router Protocol (HSRP) f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych: - SNMP (trap, probe) - WMI Performance Counters - Log Files (text, text CSV) - Windows Events (logi systemowe) - Windows Services - Windows Performance Counters (perflib) - WMI Events - Scripts (wyniki skryptów, np.: WSH, JSH) - Unix/Linux Service - Unix/Linux Log g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów 4. Tworzenie reguł a. w systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych: - Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event) - Performance based (SNMP performance, WMI performance, Windows performance) - Probe based (scripts: event, performance) b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia. c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości: - na ilość takich samych próbek o takiej samej wartości - na procentową zmianę od ostatniej wartości próbki. d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia” się monitorowanego parametru w zakresie

	przebiegu bazowego „baseline” w zadanym okresie czasu. e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji. f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym: - ASP .Net Application - ASP .Net Web Service - OLE DB - TCP Port - Web Application - Windows Service - Unix/Linux Service - Process Monitoring Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji. h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp…) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu). i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych. j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostepność), i licznika wydajności (z agregacją dla wartości – min, max, avg). 5. Przechowywanie i dostęp do informacji a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach,

	alarmy, itp…) powinny być przechowywane w bazie danych operacyjnych. b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane. c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy). d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności. e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych. f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów: - XML - CSV - TIFF - PDF - XLS - Web archive 6. Konsola systemu zarządzania a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli. b. System powinien udostępniać dwa rodzaje konsoli: - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna) - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa). c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach: - Alerts - Events - State

	- Performance - Diagram - Task Status - Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu). d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie. e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp…), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych". f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu. g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym: - opcji definiowania ról użytkowników - opcji definiowania widoków - opcji definiowania i generowania raportów - opcji definiowania powiadomień - opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących - opcji instalacji/deinstalacji klienta h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostepu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego). 7. Wymagania dodatkowe a. System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na: - Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo), - Wykonywanie operacji w systemie z poziomu linii poleceń, - Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów

	informatycznych niewspieranych natywnie przez system zarządzania, - Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyswietlanie ich stanu na diagramie, **System zarządzania środowiskami wirtualnym** System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy: 1. Architektura a. System zarządzania środowiskiem wirtualnym powinien składać się z: - serwera zarządzającego, - relacyjnej bazy danych przechowującej informacje o zarządzanych elementach, - konsoli, instalowanej na komputerach operatorów, - portalu self-service (konsoli webowej) dla operatorów „departamentowych”, - biblioteki, przechowującej komponenenty niezbędne do budowy maszyn wirtualnych, - agenta instalowanego na zarządzanych hostach wirtualizacyjnych, - „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych. b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over). c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców. 2. Interfejs użytkownika a. Konsola musi umożliwiać wykonywanie codziennych zadań związnych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny. b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień posczególnym operatorom do grup hostów. c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp... d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną,

	stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit. e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań. 3. Scenariusze i zadania a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach: 1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny, 2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych: - profilu sprzętowego - profilu systemu operacyjnego, - przygotowanych dysków twardych, b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania. c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami: - w trybie migracji „on-line" – bez przerywania pracy, - w trybie migracji „off-line – z zapisem stanu maszyny d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami. e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta. f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance" w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu. g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej. h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w

	sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji. 4. Wymagania dodatkowe a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę. b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania. c. System musi kreować raporty z działania zarządzanego środowiska, w tym: - utylizacja poszczególnych hostów, - trend w utylizacji hostów, - alokacja zasobów na centra kosztów, - utylizacja poszczególnych maszyn wirtualnych, - komputery-kandydaci do wirtualizacji d. System musi umożliwiać skorzystanie z szablonów: - wirtualnych maszyn - usług oraz profili dla: - aplikacji - serwera SQL - hosta - sprzętu - systemu operacyjnego gościa e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów). f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej. g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją) **System tworzenia kopii zapasowych** System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania: 1. System musi składać się z:

	a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych b. agentów kopii zapasowych instalowanych na komputerach zdalnych c. konsoli zarządzającej d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service) 2. System kopii zapasowych musi umożliwiać: a. zapis danych na puli magazynowej złożonej z dysków twardych b. zapis danych na bibliotekach taśmowych 3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej. 4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe. 5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej. 6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania. 7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii. 8. System kopii zapasowych powinien umożliwiać przywrócenie: a. danych plikowych b. danych aplikacyjnych c. stanu systemu (Systemstate) d. obrazu systemu operacyjnego (tzw. Bare Metal Restore) 9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych 10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości

	11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy 12. System kopii zapasowych musi rozpoznawać aplikacje: a. ze względu na tworzone logi transakcyjne: - Microsoft Exchange Server - Microsoft Office Sharepoint Server - Microsoft SQL Server b. ze względu na zapewnienie nieprzerwalności pracy - Microsoft Virtual Server 2005 - Microsoft Hyper-V server 13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach 14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach 15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów 16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń 17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje” 18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych 19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych 20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.). 21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej conajmniej do 1 roku 22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat 23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie

	te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób. 24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe. 25. System kopii zapasowych musi umożliwiać odtworzenie danych do: a. lokalizacji oryginalnej b. lokalizacji alternatywnej c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych **System automatyzacji zarządzania środowisk IT** System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk. 1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie. 2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT. 3. System musi wspomagać planowanie i automatyzację wdrażania poprawek. 4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych. 5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania worklow. 6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, IBM Tivoli i BMC Patrol do zarządzania oprogramowaniem i sprzętem. 7. Wbudowane (gotowe) workflow, takie jak: - Active Directory Password Reset - Microsoft Cluster Patching - Microsoft SQL Server Cluster Patching - Microsoft SQL: Server Dump Copy Load - Operations Manager Event Remediation - Operations Manager Event Remediation and Enrichment - Operations Manager Service Alert Testing - VM Provisioning - Working with FTP - Operations Manager Tool Integration

	- Operations Manager: Manager of Managers - Operations Manager: Maintenance Windows - Active Directory: New Employee Onboarding - Operations Manager: Multi-Service Desk Integration **System zarządzania incydentami i problemami** System zarządzania incydentami i problemami musi spełniać następujące wymagania: 1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna) 2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą. 3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami. 4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie. 5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać: - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką, - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia, - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu, - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania, - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów, - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej, - Tworzenie baz wiedzy na temat rozwiązywania problemów,

	- Automatyzację działań w przypadku znanych i opisanych problemów, - Wykrywanie odchyleń od założonych standardów ustalonych dla systemu. **Ochrona antymalware** Oprogramowanie antymalware musi spełniać następujące wymagania: 1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day. 2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem 3. Centralne zarządzanie politykami ochrony. 4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony. 5. Mechanizmy wspomagające masową instalację. 6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów", skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego. 7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania. 8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia. 9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty

	mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.). 10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania. 11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji. **System operacyjny dla serwerów** Licencja na serwerowy system operacyjny musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 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 conajmniej 64 procesorów wirtualnych oraz minimalnie 1TB pamięci RAM i dysku o pojemności conajmniej 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z minimalnie 64 węzłów, z możliwością uruchamiania conajmniej 7000 maszyn wirtualnych.

	4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

	12. Możliwość 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: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

	25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

	iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wsparcie dla algorytmów Suite B (RFC 4869), l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych

	dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
Wdrożenie	Zamawiający wymaga następujących usług wdrożeniowych: • Stworzenie dodatkowej nowej wirtualnej instancji serwera DPM z udziałem aktualnie wykorzystywanej macierzy Dell MD3200.Wykonanie backupu wszystkich maszyn wirtualnych i fizycznych serwerów. • Reinstalacja systemu operacyjnego na serwerze Dell R310 Instalacja oprogramowania do tworzenia kopi zapasowych na serwerze DPM01 do najnowszej zakupionej wersji. Reinstalacji systemu można dokonać dopiero po upewnieniu się, iż wykonały się kopie zapasowe na drugim serwerze, wirtualnym. Serwer Dell R310 z udziałem Iomega PX6-300d. Serwer ten będzie wstawiony w innej lokalizacji niż Centrala MOPS dla tego też połączenie musi być szyfrowane.

	• Kopia zapasowa całości środowiska wirtualnego oraz fizycznego.
	• Uaktualnienie środowiska wirtualnego do nowo zakupionej wersji oprogramowania. Uaktualnienie nie może powodować przestojów w pracy maszyn wirtualnych Zamawiającego.
	• Testy poprawności działania klastra wirtualizacji – testy powinny być wykonane poza godzinami pracy centrali jak i oddziałów terenowych MOPS w wyznaczonym przez zamawiającego oknie serwisowym.
	• Uaktualnienie/Wystawienie, 2 nowych maszyn wirtualnych kontrolerów domeny oraz serwerów fizycznych starego klastra do najnowszej wersji nowo zakupionych systemów operacyjnych
	• Usunięcie starych kontrolerów domeny – w wersjach starszych niż najnowsza aktualnie obowiązująca
	• Uruchomienie narzędzia do obsługi co najmniej 10 VDI
	• Uaktualnienie roli/Wystawienie nowego serwera WSUS do najnowszej wersji wraz z testami poprawności działania,
	• Repartycjonowanie usług na maszynach wirtualnych, w szczególności:
	  ○ stworzenie nowego klastra serwerow DHCP z funkcjonalnością obsługi puli adresów IP poprzez wszystkie węzły klastra
	  ○ migracja istniejącego serwera WSUS do najnowszej wersji oprogramowania
	• Testy poprawności działania maszyn wirtualnych – w szczególności serwera WDS, WSUS oraz klastra DHCP. Zamawiający wymaga raportu stanu aktualizacji systemów dla wszystkich komputerów w domenie Active Directory oraz uruchomienia testowego instalacji oprogramowania z serwera WSUS dla 5-ciu losowo wybranych komputerów z różnymi OS
	• Szkolenie administratorów do obsługi nowego środowiska, Zamawiający wymaga przynajmniej 2 dni szkoleniowych.

Dyski do Storage Iomega PX6-300d – 6szt.

Dysk twardy o pojemności nie mniejszej niż 6TB pasujące do Storage Iomega PX6-300d (np. WD RED 6TB WD60EFRX) – gwarancja nie krótsza niż 3 lata.