załącznik nr 1 do SWZ

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Jakiekolwiek nazwy własne użyte w SWZ w zakresie wszystkich części są tylko przykładami pożądanej przez Zamawiającego konfiguracji produktów, które spełniają wymogi Zamawiającego i będą kompatybilne z użytkowanym sprzętem oraz oprogramowaniem w Urzędzie Miasta Częstochowy. Zamawiający dopuszcza dostawę sprzętu i oprogramowania równoważnego, jednakże zastrzega sobie prawo do przeprowadzenia testów kompatybilności z istniejącym sprzętem oraz oprogramowaniem. Przez produkt równoważny Zamawiający rozumie produkt o parametrach i standardach jakościowych takich samych bądź lepszych w stosunku do produktów wskazanych (pożądanych) przez Zamawiającego.

Zgodnie z art. 101 ust. 4 ustawy Pzp w sytuacji, gdyby w dokumentach opisujących przedmiot zamówienia, zawarto odniesienie do norm, ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, a takim odniesieniom nie  towarzyszyło wyrażenie „lub równoważne”, to Zamawiający dopuszcza rozwiązania równoważne opisywanym w każdej takiej normie, ocenie technicznej, aprobacie, specyfikacji technicznej, systemowi referencji technicznych. W związku z powyższym należy przyjąć, że każdej: normie, ocenie technicznej, aprobacie, specyfikacji technicznej, systemowi referencji technicznych występujących w opisie przedmiotu zamówienia towarzyszą wyrazy „lub równoważne”.

Zgodnie z art. 101 ust. 5 Pzp wykonawca, który powołuje się na rozwiązania równoważne opisywanym w tych dokumentach, jest obowiązany udowodnić, poprzez dołączenie do oferty stosownych przedmiotowych środków dowodowych, o których mowa w art. 104–107 ustawy Pzp, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

Oferując produkt równoważny Wykonawca będzie zobowiązany wskazać nazwę sprzętu (typ, producenta), który oferuje oraz przedstawić w ofercie dokładny opis techniczny oferowanych zamienników, podając ich parametry techniczne.

**CZĘŚĆ 1: Zakup i dostawa zestawów komputerowych**

|  |  |
| --- | --- |
| **Zestaw komputerowy typu All in One – 250 sztuk** | |
| Procesor | Osiągający w teście PassMark Performance wynik nie niższe niż:  Single Thread Performance Passmark CPU Mark – 2700  High End CPUs Passmark CPU Mark – 6500  z wykluczeniem użycia tzw. Overclockingu. W ofercie podać wynik dla oferowanego procesora określony na podstawie średnich pomiarów opublikowanych na stronie <http://www.cpubenchmark.net/> dla zaoferowanego procesora lub wynik uzyskany na oferowanym komputerze z zainstalowanym systemem operacyjnym Microsoft Windows® 10Pro 64-Bit PL. W przypadku dokonania pomiaru wynik podać, jako średnią uzyskaną w 3 kolejno przeprowadzonych próbach.  Do oferty przetargowej załączyć wydruk ze wskazanej strony Internetowej/wydruk przeprowadzonego testu potwierdzający powyższe. |
| Pamięć RAM | 16 GB DDR4 |
| Maksymalna obsługiwana ilość pamięci RAM | 32 GB |
| Typ ekranu | Matowy, LED, IPS |
| Przekątna ekranu | 23,8" |
| Rozdzielczość ekranu | 1920 x 1080 (FullHD) |
| Karta graficzna (zintegrowana) | Osiągająca w teście PassMark- G3D Mark wynik min. 1300 pkt., z wykluczeniem użycia tzw. Overclockingu. W ofercie podać wynik dla oferowanego procesora określony na podstawie średnich pomiarów opublikowanych na stronie <http://www.videocardbenchmark.net>, dla zaoferowanej karty graficznej lub wynik uzyskany na oferowanym komputerze z zainstalowanym systemem operacyjnym Microsoft Windows® 10 Pro 64-Bit PL. W przypadku dokonania pomiaru wynik podać, jako średnią uzyskaną w 3 kolejno przeprowadzonych próbach.  Do oferty załączyć wydruk ze wskazanej strony Internetowej/wydruk przeprowadzonego testu potwierdzający powyższe. |
| Wielkość pamięci karty graficznej | Pamięć współdzielona |
| Dysk SSD | Tak, min. 250 GB |
| Napęd optyczny | Tak (DVD), (dopuszczone rozwiązanie na USB) |
| Dźwięk | Wbudowany mikrofon |
|  | Zintegrowana karta dźwiękowa |
|  | Wbudowane głośniki stereo |
| Kamera internetowa | Tak |
| Łączność | Wi-Fi |
|  | LAN 10/100/1000 Mbps |
| Złącza - panel przedni | USB – min. 1 szt. |
|  | Wyjście słuchawkowe/wejście mikrofonowe - 1 szt. |
| Złącza - panel tylny | USB - 4 szt. |
|  | RJ-45 (LAN) - 1 szt. |
|  | DC-in (wejście zasilania) - 1 szt. |
| Obudowa | Typu All in ONE |
| Dodatkowe informacje | Mysz i klawiatura w zestawie z logiem producenta komputera |
|  | Klawiatura przewodowa |
|  | Mysz przewodowa |
| Dołączone akcesoria | Kabel zasilający, Zasilacz |
| Zainstalowany system operacyjny | Licencja dla Windows 10 PRO 64 bit (preinstalowany na dysku twardym) wraz z nośnikiem pozwalającym na ponowna instalację systemu niewymagającą wpisywania klucza rejestracyjnego lub rejestracji poprzez Internet czy telefon lub oprogramowanie równoważne.  Oprogramowanie równoważne musi posiadać następujące cechy:  zgodność z interfejsem API systemu minimum Windows 7 Pro,  możliwość uruchamiania oprogramowania przeznaczonego do pracy na platformie Windows 32 bitowego bez dodatkowego oprogramowania pośredniczącego, możliwość centralnego zarządzania systemem operacyjnym bez dodatkowego oprogramowania za pomocą usług katalogowych opartych na protokole LDAP kompatybilnych ze strukturą zarządzania opartą na serwerze domenowym Windows 2003.  W przypadku dostarczenia oprogramowania równoważnego należy zapewnić odpowiednie szkolenia dla użytkowników i administratorów.  Potwierdzeniem kompatybilności oferowanej jednostki z systemem operacyjnym będzie załączony do oferty certyfikat zgodności MS WHCL. |
| Dołączone oprogramowanie | Nośnik z systemem MS Windows 10 Pro PL 64bit (dopuszczalna ukryta partycja) |
| Gwarancja | 3-letnia gwarancja door to door. Czas reakcji Wykonawcy na zgłoszenie reklamacyjne najpóźniej następnego dnia roboczego. Odbiór wadliwej stacji roboczej na koszt Wykonawcy z siedziby Zamawiającego. Czas naprawy max. 3 dni robocze lub dostarczenie sprzętu zastępczego o nie gorszych parametrach technicznych.  Diagnostyka awarii nie należy do obowiązku Zamawiającego, powinna być przeprowadzona przez autoryzowany serwis producenta sprzętu. Diagnostyka realizowana w miejscu instalacji sprzętu.  W przypadku awarii stacji roboczej/dysku twardego w okresie gwarancji, dyski pozostają u Zamawiającego — wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.  Wykonawca w przypadku wymiany części lub stacji roboczej na nowe udziela odpowiednio nowej gwarancji na daną część lub stację roboczą.  Wykonawca wymieni nieodpłatnie sprzęt na wolny od wad, po trzykrotnych naprawach gwarancyjnych tego samego egzemplarza sprzętu. Wymiana nastąpi w terminie 14 dni od dnia poinformowania pisemnego powyższym Wykonawcy przez jednostkę organizacyjną Urzędu Miasta Częstochowy |

**CZĘŚĆ 2: Rozbudowa istniejącego systemu pamięci masowych.**

**Rozbudowa istniejących macierzy EMC Unity 300 – 2 sztuki**

**(lokalizacja ul. Śląska 11/13 i Waszyngtona 5) o dodatkowe półki dyskowe wraz z dyskami**

Aktualnie użytkowane środowisko pamięci masowych składa się z dwóch replikujących się macierzy EMC Unity 300 (w lokalizacji ul. Śląska 11/13 i ul. Waszyngtona 5) wyposażonych w cztery półki, o pełnym obłożeniu dyskami.

Zadanie polega na rozbudowie obydwu macierzy poprzez zakup i instalację dodatkowej półki dla każdej z macierzy wyposażoną w 10 szt. dysków 2.5” SAS 10k o pojemności 1.8TB każdy. Pojedyncza półka musi posiadać min. 24 sloty na instalację dysków 2.5”.

Oferowane dyski do rozbudowy muszą być objęte co najmniej 3-letnim wsparciem producenta sprzętu w trybie czasu reakcji NBD (Next Business Day) w miejscu instalacji sprzętu. Dostarczone dyski wewnętrzne muszą być objęte opieką serwisową producenta przez okres 3 lat.

W okresie opieki wymagany jest bezpłatne usuwanie awarii. Dostarczone dyski muszą być objęte programem „zachowaj dysk” tzn. w przypadku awarii dysku po jego wymianie dysk pozostaje własnością zamawiającego. Wykonawca dostarczy i zainstaluje dyski w siedzibie Zamawiającego we wskazanych przez niego lokalizacjach.

W ramach zamówienia Zamawiający wymaga przedłużenia gwarancji producenta oraz wsparcia technicznego producenta dla obydwu macierzy do dnia 30 listopada 2024. Zamawiający wymaga wparcia Prosupport NBD wraz z opcją zachowania dysków twardych w razie awarii. (KEEP YOUR COMPONENT FOR ENT UNITY)

Wszystkie operacje wykonywane w ramach rozbudowy muszą odbywać się w obecności wyznaczonych pracowników Urzędu Miasta Częstochowy. Operacje wykonywane w ramach rozbudowy nie mogą powodować przerw w dostępności jakichkolwiek zasobów teleinformatycznych Zamawiającego, w szczególności systemów informatycznych, serwerów, macierzy, wewnętrznych sieci LAN/SAN itp. w godzinach pracy Urzędu Miasta Częstochowy. Rozbudowa środowiska produkcyjnego nie może spowodować jakiejkolwiek utraty danych lub awarii w infrastrukturze informatycznej Zamawiającego.

Wykonawca skonfiguruje urządzenia do udostępniania zasobów w sposób wskazany przez Zamawiającego oraz uruchomi replikację pomiędzy rozbudowanymi przestrzeniami. Po zakończeniu prac, potwierdzonych protokołem odbioru, Wykonawca sporządzi i przekaże dokumentację techniczną dla wdrożonej rozbudowy nie później niż 30 dni od podpisania protokołu odbioru.

**CZĘŚĆ 3: Rozbudowa istniejącego środowiska wirtualizacyjnego o dwa serwery backupu i licencje do środowiska wirtualizacyjnego oraz systemu backup’owego Avamar**

1. **Rozbudowa istniejącego środowiska wirtualizacyjnego o serwery backupu oraz licencje**

Aktualnie użytkowane środowisko wirtualizacyjne składa się z klastra obejmującego trzy serwery Dell PowerEdge R630 zainstalowanym oprogramowaniem VMware ESXi 6.5.0 oraz cztery serwery Dell PowerEdge R640 zainstalowanym oprogramowaniem VMware ESXi 6.5.0. Do zarządzania całością środowiska wirtualnego wykorzystywane jest oprogramowanie Vmware vSphere w wersji 6.5.

Zadanie Wykonawcy polega na:

* rozbudowie środowiska wirtualnego o dwa serwery stanowiące hosty wirtualizacje zgodne ze specyfikacją tabela nr 1, podłączenie i skonfigurowanie z istniejącym środowiskiem wirtualizacyjnym zgodnie z wytycznymi Zamawiającego,
* dostarczenie licencji systemu wirtualizacyjnego zgodnego z aktualnie wykorzystywanym systemem przez Zamawiającego obejmującej dostarczone serwery. Dostarczone oprogramowanie wirtualizacyjne musi w pełni wykorzystywać funkcjonalności środowiska pamięci masowych oraz systemu kopii zapasowych (m.in. bezpośredni dostęp i możliwość uruchomienia maszyny wirtualnej z snapshotu przechowywanego na macierzach oraz systemie kopii zapasowych),
* licencje na system istniejącego środowiska wirtualizacyjnego wraz z dostarczoną licencją obejmującą dostarczone hosty, muszą być objęte serwisem producenta na okres 3 lat , do dnia 30 listopada 2024 roku (możliwość aktualizacji oprogramowania do najnowszej wersji) od daty podpisania protokołu odbioru,
* aktualizacja całego środowiska wirtualnego do ostatniej stabilnej wersji zalecanej przez producenta oprogramowania,

lub dostarczenie rozwiązania równoważnego zgodnego z tabelą 2 wraz z przeniesieniem środowiska produkcyjnego Zamawiającego na nowe rozwiązanie – bez przestojów w pracy Zamawiającego oraz z szkoleniami 4 administratorów.

Wykonawca dostarczy i zainstaluje urządzenia w siedzibie Zamawiającego we wskazanych przez niego lokalizacjach. **Wszystkie operacje wykonywane w ramach rozbudowy muszą odbywać się w obecności wyznaczonych pracowników Urzędu Miasta Częstochowy. Operacje wykonywane w ramach rozbudowy i integracji nie mogą powodować przerw w dostępności jakichkolwiek zasobów teleinformatycznych Zamawiającego, w szczególności systemów informatycznych, serwerów, macierzy, wewnętrznych sieci LAN/SAN itp. w godzinach pracy Urzędu Miasta Częstochowy. Rozbudowa środowiska produkcyjnego nie może spowodować jakiejkolwiek utraty danych lub awarii w infrastrukturze informatycznej Zamawiającego. Wykonawca skonfiguruje urządzenia w sposób wskazany przez Zamawiającego** Po zakończeniu prac, potwierdzonych protokołem odbioru, Wykonawca sporządzi i przekaże dokumentację techniczną dla wdrożonej rozbudowy nie później niż 30 dni od podpisania protokołu odbioru.

**Tabela nr 1 – wymagania serwerów**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka** |
| **Obudowa** | Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli, z możliwością instalacji min. 16 dysków 2.5" Hot-Plug. Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Zainstalowane dwa procesory ośmio-rdzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 120 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów.  Wydruk testów należy dołączyć do oferty przetargowej. |
| **RAM** | 64GB DDR4 RDIMM min. 3200MT/s, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror |
| **Gniazda PCI** | min. 3 sloty PCIe Gen. 3 |
| **Interfejsy sieciowe** | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T oraz 2 porty 10Gb BaseT  Zainstalowana karta FC dwuportowa 16Gb/s  Możliwość zainstalowania:   * karty 10GbE w standardzie SFP+ * karty FC min. 8Gb/s.   Karta sieciowa (moduł) osadzona na płycie głównej serwera, nie zajmująca dodatkowych gniazd PCI Express. |
| **Inne** | 2 kable miedziane typu Direct-Attach o przepustowości 10GbE i minimalnej długości 10 metrów z zainstalowanymi modułami SFP+ 10GbE kompatybilnymi z gniazdami SFP+ zaoferowanych urządzeń oraz kompatybilnymi z posiadanymi przez Zamawiającego urządzeniami Cisco Catalyst WS-C4500X-32SFP+ |
| **Napęd optyczny** | Brak napędu DVD-ROM |
| **Dyski twarde** | Zainstalowane min 12 x 2.4TB SAS o prędkości 10k z interfejsem min. SAS 12Gb/. oraz 1 dysk min. 480GB SSD.  Zainstalowany wewnętrzny moduł dedykowanego dla hypervisora wirtualizacyjnego, wyposażony w 2 jednakowe nośniki typu flash o pojemności minimum 16GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy.  Możliwe konfiguracje poziomów RAID: 1, 5, 10, 50 |
| **System operacyjny** | Brak systemu operacyjnego. |
| **Wbudowane porty** | Minimum 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty RJ45, 1 port VGA, 1 port RS232 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024. |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Redundantne, Hot-Plug nie więcej niż 750W każdy. |
| **Bezpieczeństwo** | Zintegrowany z płytą główną moduł TPM w wersji minimum 1.2  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet 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 podłączenia lokalnego poprzez złącze RS-232 * możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.   Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów– WMI, SNMP, IPMI, , Linux SSH * Możliwość oskryptowywania procesu wykrywania urządzeń * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS * Grupowanie urządzeń w oparciu o kryteria użytkownika * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych * Możliwość automatycznego przywracania ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 lub równoważny oraz ISO-14001 lub równoważny.  Serwer musi posiadać deklaracja CE.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2, Windows Server 2016. |
| **Warunki gwarancji** | Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.  W przypadku awarii dyski twarde pozostają własnością zamawiającego – do oferty dołączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku  Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. |
| **Dokumentacja użytkownika** | Wymaga się dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

**Tabela nr 2 – wymagania oprogramowania wirtualizacyjnego:**

|  |
| --- |
| Zamawiający wymaga obłożenie licencjami dostarczonego hostu 2 procesorowego.  **Specyfikacja wirtualizatora:**   1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. 4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. 6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych  z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych ,z których każda może mieć 1-10 wirtualnych kart sieciowych. 9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych , z których każda może mieć 32 porty szeregowe. 10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 12. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM. 13. Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 14, Ubuntu 12, SCO OpenServer, SCO Unixware, Mac OS X. 14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. 16. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. 17. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. 18. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 19. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 20. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 21. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. 22. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych. 23. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. 24. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. 25. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. 26. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. 27. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory. 28. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 29. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. 30. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). |

1. **Rozbudowa posiadanych licencji EMC Avamar o obsługę dodatkowych pojemności na deduplikaty.**

Przedmiotem zamówienia jest:

* oprogramowanie tworzące SYSTEM OCHRONY DANYCH w skład którego wchodzi:
  + aplikacja backup’owa
  + system raportujący
  + system dedykowany do wyszukiwania danych
  + system umożliwiający zabezpieczenie danych w trybie Continuous Data Protection
  + system umożliwiający instalację oraz eksploatację deduplikatora
  + system umożliwiający zarządzanie SYSTEMEM OCHRONY DANYCH

Poniższe zestawienie obejmuje wymagane funkcjonalności oprogramowania dedykowanego do stworzenia SYSTEMU OCHRONY DANYCH

|  |  |  |
| --- | --- | --- |
|  | Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu do zabezpieczania środowiska Data Center (baz danych, maszyn wirtualnych, serwerów wolnostojących). |  |
|  | Wymagane jest dostarczenie modułów oprogramowania:  backupowego (aplikacja backupowa)  umożliwiającego stworzenie systemu raportującego  umożliwiającego zaindeksowanie oraz przeszukiwanie danych backupowych  umożliwiającego stworzenie rozwiązania Continuous Data Protection (CDP) dla środowisk VMware  umożliwiającego konfigurację/instalację deduplikatora  umożliwiające zarządzanie oferowanym środowiskiem dedykowanym do zabezpieczania danych  oferowane oprogramowanie powinno spełniać wszystkie wymienione w niniejszej tabeli funkcjonalności. Wymagane wsparcie na oferowane oprogramowanie realizowane przez producenta w okresie min. 3 lata w trybie 9x5 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania. | 3 lata/ 36 miesiący |
|  | Wymagane jest dostarczenie licencji w/w oprogramowania do zabezpieczania danych dla środowiska obejmującego zarówno serwery niezwirtualizowane oraz zwirtualizowane, charakteryzujące się sumaryczną ilością: 20 CPU. Zamawiający przewiduje w kolejnych latach rozbudowę zabezpieczanego środowiska, dlatego wymagana jest możliwość skalowania rozwiązania stworzonego w oparciu o licencje będące przedmiotem zapytania - poprzez dokładanie kolejnych licencji, co powinno umożliwić zabezpieczenie środowiska o sumarycznej ilości 50 CPU, bez względu na rozmiar zabezpieczanego wolumenu danych. Licencje będące przedmiotem zapytania powinny umożliwić skonfigurowanie na zaoferowanych serwerach deduplikatora o sumarycznej pojemności nie mniejszej niż 40TB netto oraz umożliwić zabezpieczenie dowolnej ilości maszyn wirtualnych (min. vSphere 6.5) w trybie CDP. | 4 procesory |

**Wymagania dotyczące aplikacji backupowej:**

|  |  |  |
| --- | --- | --- |
| 1 | Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubuntu), Solaris, AIX, HP-UX, FreeBSD.  Backup zasobów plików w przypadku powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami. |  |
|  | Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, IBM DB2, Lotus Notes, SharePoint, SAP, Sybase, VMware vSphere, Hyper-V.  Backup powyższych baz danych i aplikacji musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami. |  |
|  | W przypadku zabezpieczania baz danych i aplikacji wymagana możliwość realizacji kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni). |  |
|  | Zabezpieczane serwery muszą być backupowane bezpośrednio na dyski de-duplikatora (zainstalowanego/skonfigurowanego w oparciu o licencje będące przedmiotem zapytania) bez pośrednictwa jakichkolwiek innych urządzeń/serwerów, dostarczone licencje (dotyczy aplikacji backup’owej oraz deduplikatora) powinny umożliwiać całkowitą utylizację wymaganej przestrzeni deduplikatora. |  |
|  | Transfer danych z zabezpieczanych serwerów do oferowanego de-duplikatora nie może się odbywać po sieci SAN. |  |
|  | Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej:   * + backup pojedynczych plików   + backup całych systemów plików   + backup baz danych w trakcie ich normalnej pracy   + backup ustawień systemu operacyjnego Windows.   + backup całych obrazów maszyn wirtualnych systemu VMware vSphere   + backup całych obrazów maszyn wirtualnych systemu Hyper-V |  |
|  | Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio ze zdalnych oddziałów do oferowanych deduplikatora bez konieczności instalacji jakiegokolwiek sprzętu w oddziale. Powyższa funkcjonalność wymagana jest dla następujących typów danych:   * + backup pojedynczych plików   + backup całych systemów plików   + backup baz danych w trakcie ich normalnej pracy |  |
|  | W przypadku zabezpieczania środowisk zdalnych, oferowane rozwiązanie backupowe nie może wymagać zaangażowania ze strony personelu w oddziale. |  |
|  | Wymaga się aby oferowane rozwiązanie backupowe było w pełni konfigurowalne ze zdalnej konsoli, w szczególności backupy maszyn w oddziałach (bazy, pliki) muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę. |  |
|  | Oferowane rozwiązanie backupowe musi umożliwiać odtworzenie   * + plików   + baz danych   na docelową maszynę w infrastrukturze Zamawiającego - z poziomu centralnej konsoli systemu backupowego. Wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego. |  |
|  | W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych do docelowego serwera w postaci skompresowanej, odtwarzane dane powinny zostać rozkompresowane na docelowym serwerze przez agenta oferowanego systemu. |  |
|  | Oprogramowanie backupowe musi posiadać funkcjonalność podziału danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki o różnej długości w ramach pojedynczego dokumentu w celu polepszenia efektywności deduplikacji.  Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze. |  |
|  | Używany algorytm de-duplikacji musi również generować zmienny blok w przypadku backupu pojedynczego dokumentu. Bloki wysyłane w trakcie backupu pojedynczego dokumentu (z zabezpieczanej maszyny do medium de-duplikacyjnego) muszą być różnej długości jednak nie większej niż 32kB. |  |
|  | Wymaga się aby oprogramowanie backupowe przesyłało na oferowanego deduplikatora tylko unikalne bloki nie znajdujące się na tym urządzeniu, w efekcie skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN. |  |
|  | Funkcjonalność deduplikacji nie może wymagać instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego. |  |
|  | Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być ponownie odczytywany, chyba, że zmieni się jego zawartość. |  |
|  | Wymaga się aby oprogramowanie backupowe realizowało wyłącznie - logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do oferowanych de-duplikatorów powinny być przesyłane dane po de-duplikacji, jednak każdy finalny backup musi być logicznie pełnym backupem. W wewnętrznej strukturze systemu musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach), dzięki czemu odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu. |  |
|  | Wymagana możliwość definiowania w konsoli oprogramowania backupowego ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte. |  |
|  | Wymagana możliwość tworzenia z poziomu GUI (konsoli graficznej) w przypadku oferowanego oprogramowania backupowego, polityk typu „dziadek – ojciec –syn”, to znaczy tworzenia polityk w których zdefiniowano:   * + Czas przechowywania backupów dziennych   + Czas przechowywania backupów tygodniowych   + Czas przechowywania backupów miesięcznych   + Czas przechowywania backupów rocznych |  |
|  | Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Wymagana możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:   * + wybranych typów plików, np. dla plików z rozszerzeniem mp3   + dla całych katalogów (np.: c:\windows).   + dla pojedynczych plików |  |
|  | Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie będzie backupowany w przyszłości to automatycznie ostatni ważny backup tego zasobu będzie przechowywany bezterminowo, jedynie administrator może zdecydować o jego usunięciu. |  |
|  | Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min, administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym. |  |
|  | Wymagana możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni przeznaczonej na składowanie de-duplikatów. |  |
|  | Bloki przesyłane z zabezpieczanych serwerów do oferowanego deduplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym. |  |
|  | Wymagana jest autentykacja komunikacji między klientem a serwerem backupu (farmą serwerów) oparta na certyfikatach. |  |
|  | Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, wymagane odtworzenie danych w jednym kroku. |  |
|  | Wymagana możliwość limitowania wielkości zadania backupowego, jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowym. |  |
|  | Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak aby odpowiednia moc procesora pozostała do wykorzystania dla innych zadań. |  |
|  | Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0, 6.5.  Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu:   1. Backup całych maszyn wirtualnych 2. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk 3. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane 4. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware) 5. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk)   Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z przytoczonymi wymaganiami dla deduplikacji.  Powyższe metody backupu muszą być wbudowane w oferowany system backupu, nie powinny wymagać tworzenia skryptów/dodatkowych komend. |  |
|  | Oferowany system musi pozwalać na szybkie odtworzenie   * całych obrazów maszyn wirtualnych * pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej |  |
|  | Wymaga się aby oferowane rozwiązanie backupowe umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami:   1. odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu 2. odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu 3. odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux. 4. możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows), w efekcie metoda ta nie odtwarza backupów a jedynie umożliwia na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie   Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne nie mogą generować konieczności wykorzystania dodatkowych skryptów/ komend. |  |
|  | Oferowane oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej. |  |
|  | Oferowane oprogramowanie backupowe musi mieć możliwość backupu/odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter. |  |
|  | Oferowane oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware, wymagana możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware.  Weryfikacja maszyn wirtualnych musi zapewniać minimum:   1. odtworzenie maszyny wirtualnej na zdefiniowanym Data Center/Data Store 2. weryfikację podstawowych procesów 3. możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej   Wymagana dostępność informacji w konsoli systemu backupu o statusie (poprawna/niepoprawna) weryfikacji maszyny wirtualnej. |  |
|  | Administrator (właściciel) danej maszyny wirtualnej VMware vSphere musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej. |  |
|  | Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware vSphere dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym. |  |
|  | Oferowane rozwiązanie backupowe musi umożliwiać na tworzenie automatycznych polityk backupowych dla:   * + Folderu   + Resource Pool   systemu VMware vSphere. Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware. |  |
|  | Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych. |  |
|  | Oferowany system musi automatycznie naprawiać problemy związane ze snapshotami VMware. W przypadku gdy system VMware nie usunie snapshotu, oprogramowanie backupowe musi automatycznie ponawiać usunięcie snapshotu a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware |  |
|  | Wymaga się aby inicjowanie backupu oraz odtwarzanie maszyn wirtualnych VMware dostępne było z poziomu graficznego interfejsu, linii komend oraz przez REST API |  |
|  | Oferowane oprogramowanie backupowe powinno umożliwiać dla środowisk Hyper-V:  a. backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V.  b. backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę), takie wykonanie backupu nie powinno wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd).  c. wykonywanie backupu jak w punkcie b. powinno umożliwiać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta powinna być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows.   * dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych. * powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. * powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej. |  |
|  | Oferowane oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V |  |
|  | Wymagana możliwość odtworzenia danych   * + z zabezpieczanego serwera / komputera   + z konsoli systemu backupowego |  |
|  | Wymagana możliwość odtworzenia:   * + Pojedynczego pliku   + Zabezpieczanej bazy danych |  |
|  | W przypadku systemów Windows 2012, Windows 2016 wymagana funkcjonalność Bare Metal Recovery - automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia,  Funkcjonalność ta powinna być wbudowana w rozwiązanie backupowe. |  |
|  | W przypadku odtwarzania danych poprzez interfejs dostępny na zabezpieczanym serwerze/laptopie wymagany mechanizm autentykacji użytkowników spełniający funkcjonalności:   * + mechanizm wbudowany w system backupowy   + mechanizm zintegrowany z usługami katalogowymi   + w przypadku wykorzystania AD, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności     1. odtworzenia danych     2. przeszukania zwartości swoich backupów     3. wykonania backupu |  |
|  | W przypadku odtwarzania istniejącego systemu plików (systemu plików który utracił część zasobów) oprogramowanie backupowe musi samo, automatycznie sprawdzać których plików znajdujących się w backupie, brakuje na odtwarzanej maszynie a następnie odczytać z backupu i przesłać tylko te pliki które znajdują się w backupie a których brakuje na odtwarzanej maszynie. |  |
|  | Oferowany system backupu musi być dostępny (dla backupu i odtwarzania) przez 24h na dobę 7 dni w tygodniu, wyklucza się istnienie okresów w przypadku których system backupowy nie może wykonywać backupu lub odtwarzania (tzw. BLACKOUT WINDOWS). |  |
|  | Wymaga się aby oferowany system backupu posiadał możliwość bezpośredniego raportowania o błędach do serwisu producenta |  |
|  | Oferowany system backupu powinien mieć możliwość instalacji agentów jako plików msi. Wymagana możliwość automatyzacji instalacji agentów poprzez uruchomienie skryptu na zabezpieczanej maszynie, przyporządkowującego maszynę automatycznie do określonej polityki backupowej. |  |
|  | Oferowany system backupu powinien posiadać możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji oprogramowania od producenta. |  |
|  | Oferowany system backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu. |  |

**W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów:**

|  |  |  |
| --- | --- | --- |
|  | W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów:   * 1. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)   2. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych)   3. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów   4. Zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami   5. Zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane   6. Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii)   7. Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów)   8. Lista najwolniejszych/najszybszych zabezpieczanych maszyn   9. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego   10. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się dotwarzamy)   11. Liczba danych backupowanych dziennie   12. Liczba zadań backupowych dziennie   13. Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN)   14. Zużycie mediów backupowych i napędów taśmowych   15. Aktualna konfiguracja systemu backupowego   16. Historia zmian konfiguracji systemu backupowego   17. Posiadane licencje systemu backupowego   18. Wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center) |  |
|  | W ramach dostarczonych licencji wymagana możliwość zaindeksowania oraz przeszukiwania backupów z poziomu graficznego interface’u (GUI), wymagana także możliwość wyszukania dowolnych fraz w nazwach plików. |  |

**W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk VMware**

|  |  |  |
| --- | --- | --- |
|  | integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT) , vSphere Web Client GUI |  |
|  | wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion |  |
|  | możliwość integracji z VMware vRealize Operations Manager |  |
|  | rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi |  |
|  | zabezpieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 6.0, 6.5 |  |
|  | możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM) |  |
|  | zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT’ów ) na poziomie VMDK oraz RDM, niezależnie od użytego storage’u (tzw. Storage Agnostic -warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS |  |
|  | wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska |  |
|  | odporność na krótkotrawałe problemy (przeciążenie, zaniki) związane z siecią WAN |  |
|  | wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN |  |
|  | wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP) |  |
|  | proponowane rozwiązanie powinno umożliwiać:   * stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware vSphere * operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami * MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe |  |
|  | równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection … tryb replikacji lokalnej), CRR (Continuous Remote Replication … tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication … połączenie CDP oraz CLR … tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji |  |
|  | granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją |  |
|  | architektura FAULT-TOLERANT, brak pojedynczego punktu awarii |  |
|  | działanie rozwiązania będącego przedmiotem zapytania nie może mieć negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji |  |
|  | wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund |  |
|  | proponowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa:   * RPO=30s z ostatnich 24h, * RPO=24h z ostatniego tygodnia, * RPO=1tydzień z ostatniego miesiąca |  |
|  | możliwość odtworzenia zabezpieczanego środowiska do DOWOLNEGO punktu w czasie |  |
|  | możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM) |  |
|  | rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu |  |
|  | możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji |  |
|  | wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS |  |
|  | możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację |  |
|  | możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM) |  |
|  | możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK |  |
|  | możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …) |  |
|  | możliwość skryptowego tworzenia planów RECOVERY |  |

**Wymagania funkcjonalne dotyczące deduplikatora skonfigurowanego w oparciu o dostarczone licencje (wymagany rozmiar deduplikatora został podany wcześniej)**

|  |  |  |
| --- | --- | --- |
|  | Rozwiązanie powstałe w wyniku instalacji/konfiguracji dostarczonych licencji musi być przeznaczone do deduplikacji, dedykowane do przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |  |
|  | Oprogramowanie musi umożliwiać konfigurację deduplikatora na platformie VMware vSphere 6.5 oraz Microsoft Windows Server 2012 R2 z Hyper-V, o wcześniej określonej przestrzeni (powierzchni użytkowej dedykowanej do przechowywania deduplikatów) bez uwzględniania mechanizmów protekcji, wymagane skalowanie do min. 90TB powierzchni netto w ramach tego samego urządzenia. |  |
|  | Deduplikator musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami:   * CIFS * NFS * deduplikacja na źródle (alternatywnie OST/BOOST/CATALYST)   w obrębie oferowanej pojemności urządzenia. |  |
|  | Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia. |  |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 20 strumieni |  |
|  | Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |  |
|  | Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. |  |
|  | De-duplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jakie są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia w celu maksymalnego zwiększenia efektywności deduplikacji. |  |
|  | Niedopuszczalna jest deduplikacja stałym blokiem o ustalonej tej samej długości, możliwość manulanej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest każdy strumień danych. |  |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia.  W obrębie całego urządzenia, raz otrzymany i zapisany w urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. |  |
|  | Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej deduplikacji pomiędzy dowolnymi dwoma udziałami NFS, CIFS. Blok danych otrzymany i zapisany na udział CIFS, nie może zostać ponownie zapisany jeśli trafi do udziału NFS w obrębie tego samego urządzenia (to samo dotyczy deduplikacji na źródle) |  |
|  | Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych. |  |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo skompresowane |  |
|  | Oferowane rozwiązanie musi wspierać posiadane aplikacje backupowe, EMC Networker, EMC Avamar. |  |
|  | W przypadku współpracy z każdą z poniższych aplikacji:   * RMAN (dla ORACLE) * Microsoft SQL Server Management Studio (dla Microsoft SQL) * VERITAS NetBackup * EMC NetWorker * Veeam   urządzenie musi umożliwiać de-duplikację na źródle (deduplikację na zabezpieczanej maszynie) i przesyłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do oferowanego urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. |  |
|  | W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |  |
|  | Urządzenie powinno dopuszczać co najmniej 90% utylizację powierzchni netto, bez widocznego spadku wydajności. Dokumentacja urządzenia nie może wskazywać na jakiekolwiek problemy czy obostrzenia, które mogą pojawić się przy zapełnieniu urządzenia poniżej 90%. |  |
|  | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia tego samego typu (pomiędzy oboma zaoferowanymi urządzeniami), oraz do posiadanych przez Zamawiającego urządzeń DataDomain 2200 i DataDomain 2500, wymagane następujące tryby pracy replikacji:   * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządzenia B które te same dane replikuje do urządzenia C).   Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu, rozwiązanie replikacyjne nie powinno wymagać aby obszar na który dane są replikowane był większy od obszaru źródłowego (replikowanego) w przypadku schematu „jeden do jednego” – weryfikacja na podstawie ogólnie dostępnej dokumentacji producenta oraz zaleceń. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania. |  |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |  |
|  | W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy: oferowaną aplikację backupową/ VERITAS NetBackup /EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących * replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu * replikacja zarządzana jest z poziomu aplikacji backupowej, aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |  |
|  | Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%. |  |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. |  |
|  | Deduplikator musi umożliwiać wykonywanie oraz przechowywanie SnapShot’ów (min. 50 jednocześnie), czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania). |  |
|  | Deduplikator musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia). |  |
|  | Deduplikator musi mieć możliwość podziału na minimum 14 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 14 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |  |
|  | Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |  |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego poprzez:   * CIFS * NFS * wymagany protokół umożliwiający deduplikację na źródle |  |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |  |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu), nie może wymagać (zgodnie z oficjalnymi zaleceniami producenta) definiowania BLACKOUT WINDOW czyli okna czasowego dedykowanego dla procesu czyszczenia podczas którego nie są realizowane procesy backupu / odtwarzania danych czy replikacji. |  |
|  | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). |  |
|  | Wymagana możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia). |  |
|  | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |  |
|  | Urządzenie musi mieć możliwość zarządzania poprzez   * interfejs graficzny dostępny z przeglądarki internetowej * poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |  |

**Wymagania funkcjonalne dotyczące środowiska umożliwiającego zarządzanie środowiskiem dedykowanym do zabezpieczania danych stworzonego w oparciu o oprogramowanie będące przedmiotem postępowania**

|  |  |  |
| --- | --- | --- |
|  | Możliwość uruchomienia zdalnych konsol dla:   * aplikacji backup’owej * systemu dedykowanego do raportowania * systemu dedykowanego do przeszukiwania danych backup’owych * systemu CDP * deduplikatora   stworzonych w oparciu o oprogramowanie będące przedmiotem postępowania, możliwość zdalnego uruchomienia oraz wyłączenia w/w komponentów |  |
|  | Zapewnienie podglądu on-line takich elementów jak:   * aktywność procesów backup’owych * aktywność procesów replikacyjnych * aktualny status * alarmy   w przypadku zaoferowanej aplikacji backup’owej oraz deduplikatora |  |
|  | Możliwość zarządzania procesem wyszukiwania danych backup’owych |  |
|  | Integracja z oferowanym rozwiązaniem dedykowanym do raportowania, możliwość inicjowania raportów |  |

**Wdrożenie:**

1. Instalacja i konfiguracja urządzeń fizycznych,
2. Podłączenie urządzeń do sieci LAN/SAN
3. Konfiguracja serwera backupu
   * parametry dostępu do interfejsu zarządzania serwerem
   * konfiguracja lokalnej przestrzeni dyskowej
4. Aktualizacja mikrokodu (firmware) komponentów serwerów do najnowszej zalecanej przez producenta wersji.
5. Instalacja systemu operacyjnego wirtualizatora dla systemu kopiowania i odtwarzania danych
6. Konfiguracja parametrów systemów operacyjnego (LAN), instalacja poprawek systemowych
7. Instalacja dostarczonego systemu kopiowania i odtwarzania danych jako maszyna wirtualna
8. Konfiguracja parametrów sieciowych systemu kopiowania i odtwarzania danych
9. Instalacja dostarczonego systemu składowania kopii zapasowych z funkcją deduplikacji danych jako maszyna wirtualna
10. Konfiguracja parametrów sieciowych systemu deduplikatora
11. Konfiguracja protokołów dostępowych do deduplikatora
12. Konfiguracja urządzeń składowania danych (repozytoria kopii zapasowych)
    * Przestrzenie dyskowe
    * Przestrzenie dyskowe z deduplikacją
13. Organizacja przestrzeni dyskowej na obecnie posiadanych urządzeniach przechowywania danych
14. Konfiguracja przestrzeni dyskowej dedykowanej dla składowania unikatowych bloków
15. Prezentacja danych dla systemu kopiowania i odtwarzania danych
16. Zestawienie replikacji pomiędzy wdrażanymi oraz posiadanymi rozwiązaniami
17. Konfiguracja polityk ochrony dla wskazanych maszyn wirtualnych/fizycznych:
    * Definicje typów kopii zapasowych (obraz maszyny, dane plikowe, dane aplikacyjne w trybie online, dane aplikacyjne w trybie offline)
    * Definicja harmonogramów
    * Definicja miejsc składowania kopii zapasowych
    * Definicja polityk retencji
    * Testy odtwarzania danych

W przypadku dostarczenia rozwiązania równoważnego zgodnego z powyższą specyfikacją oraz przeniesienia istniejącego środowiska produkcyjnego kopii zapasowych Zamawiającego na nowe rozwiązanie – bez przestojów w pracy Zamawiającego wymagane jest szkolenie 4 administratorów. Po zakończeniu prac, potwierdzonych protokołem odbioru, Wykonawca sporządzi i przekaże dokumentację techniczną dla wdrożonej rozbudowy systemu kopii zapasowych nie później niż 30 dni od podpisania protokołu odbioru.

**CZĘŚĆ 4: Zakup i dostawa przełączników zarządzalnych warstwy 2**

|  |  |
| --- | --- |
| **Przełącznik zarządzalny warstwy 2 - szt. 2** | |
| Porty | * 48 portów 10/100/1000 Ethernet RJ45 + PoE+ * 2 porty Uplink SFP+ z zainstalowanymi modułami światłowodowymi 10Gigabit Ethernet o zasięgu min. 10 km posiadającymi złącze typu LC oraz przystosowanymi do współpracy z światłowodami typu single-mode i kompatybilnymi z gniazdami SFP+ zaoferowanych urządzeń oraz kompatybilnymi z posiadanymi przez Zamawiającego urządzeniami Cisco Catalyst WS-C4500X-32SFP+ |
| Całkowita moc zasilania | 740W |
| Pamięć | min. 512 MB pamięci DRAM oraz  128 MB pamięci Flash |
| Wydajność przełączania | Co najmniej 216 Gbps |
| Przepustowość | Co najmniej 130 Mpps |
| Tablica MAC | Obsługa min. 16000 adresów MAC |
| Obsługa ruchu multicast | Z wykorzystaniem IGMPv3 snooping |
| Ramki Jumbo | Min. 9216 bajtów |
| Sieci VLAN | * obsługa co najmniej 1000 sieci VLAN i 4000 VLAN ID * obsługa mechanizmów dystrybucji informacji o sieciach VLAN pomiędzy przełącznikami |
| Wsparcie dla protokołów | * IEEE 802.1w * IEEE 802.1s * IEEE 802.3ad * IEEE 802.1x |
| Bezpieczeństwo | * Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL * Obsługa funkcji Guest VLAN * Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC * Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez obsługi protokołu 802.1X * Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www * wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie |
| Jakość usług | * Wsparcie dla IEEE 802.1p * Obsługa min. 4 kolejek priorytetów na każdym porcie wyjściowym |
| Zarządzanie | * Zarządzanie przez SNMP v1/v2/v3 * Zarządzanie przez przeglądarkę WWW – protokół http i https * Zarządzanie przez TELNET * Zarządzanie przez CLI * Zarządzanie przez port szeregowy * Obsługa protokołu NTP * Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB |
| Możliwość montażu w szafie 19” | Tak |
| Zasilanie | Możliwość zastosowania redundantnego zasilacza |
| Dodatkowe wyposażenie | Dwa podwójne patchordy światłowodowe typu single-mode ze złączami typu  LC/PC-E2000/APC o długości min. 3m |
| Kompatybilność z posiadanymi urządzeniami | Zamawiający wymaga aby dostarczone urządzenia były kompatybilne na poziomie protokołów sieciowych z posiadanymi przez Zamawiającego urządzeniami Cisco Catalyst WS-C4500X-32SFP+ stanowiącymi rdzeń sieci komputerowej. |
| Gwarancja | * Okres gwarancji – 36 miesięcy/3 lata * Czas naprawy – 24 godziny od momentu zgłoszenia uszkodzenia bądź dostawa w ciągu 24 godzin sprzętu zastępczego o parametrach nie gorszych niż sprzęt uszkodzony |