Załącznik nr 1b do SIWZ
Modyfikacja z dnia 30 czerwca 2020 r.

OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy postępowania o udzielenie zamówienia publicznego na:

„Wyposażenie serwerowni Centrum Komiksu i Narracji Interaktywnej"
Numer postępowania: 206/DIM/PN/2020

Zadanie 2

Dostawa serwerów, macierzy oraz oprogramowania wraz z wdrożeniem, konfiguracją i uruchomieniem

Spis treści

1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. Dostawa wraz z wdrożeniem kompletnego rozwiązania składającego się z:
    a. 2 serwerów fizycznych,
    b. 1 macierzy dyskowej,
    c. 1 systemu do wirtualizacji,
    d. 1 systemu do wykonywania kopi zapasowych,
    e. 4 przełączników sieciowych 10 Gbps,
    f. 2 dodatkowych modułów switch'a Aruba;
2. Wdrożenie obejmujące elementy wskazane w pkt. 1;
3. Instruktaż dla administratorów;
4. Przygotowanie dokumentacji powdrożeniowej.

2. Serwer fizyczny

2.1. Wymagania dotyczące parametrów serwera fizycznego

Parametr	Wymagania minimalne
Obudowa	Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
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 min. ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 83.3 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	Minimum 256GB DDR4 RDIMM 2933MT/s, na płycie głównej powinny znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	Minimum trzy sloty PCIe x16 generacji 3 połowy wysokości
Interfejsy sieciowe /FC/SAS	Wbudowane min. cztery interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+. Możliwość instalacji wymiennie modułów udostępniających:

	- dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+; - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT; - cztery interfejsy sieciowe 1Gb Ethernet w standardzie SFP+; - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.
Dyski twarde	Obudowa serwera z możliwością zamontowania do 8 dysków twardych 2.5“. Zainstalowane 2 dyski twarde 480GB SSD SATA typu Read Intensive 2.5“. Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 16GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID 1.
Kontroler RAID	Wbudowany kontroler SATA
Wbudowane porty	4 x USB z czego nie mniej niż 1 na przednim panelu obudowy i jeden wewnętrzny, 4 x SFP+, 2xVGA z czego jeden na panelu przednim, 1xRS-232.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 750W każdy.
Bezpieczeństwo	Zintegrowany moduł TPM 1.2. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port RJ-45 Gigabit Ethernet, umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - szyfrowane połączenie (TLS) oraz autentykację 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, SSH - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer - integracja z Active Directory - możliwość obsługi przez ośmiu administratorów jednocześnie - wsparcie dla automatycznej rejestracji DNS

	- wsparcie dla LLDP - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej - możliwość podłączenia lokalnego poprzez złącze RS-232 - możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy - monitorowanie zużycia dysków SSD - możliwość monitorowania z jednej konsoli min. 100 serwerów fizycznych, - automatyczne zgłaszanie alertów do centrum serwisowego producenta - automatyczny update firmware dla wszystkich komponentów serwera - możliwość przywrócenia poprzednich wersji firmware - możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON - możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych - automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram - karta z możliwością wyposażenia we wbudowaną wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 bądź równoważnymi. Serwer musi posiadać deklarację 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 x64, Microsoft Windows 2016.
Warunki gwarancji	Okres gwarancji producenta, jednak nie krótszy niż zadeklarowany w ofercie. Serwis gwarancyjny realizowany w miejscu instalacji sprzętu z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta/wykonawcy lub dedykowaną stronę www producenta/wykonawcy.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

3. Macierz dyskowa:

3.1. Wymagania dotyczące macierzy dyskowej

Parametr	Wymagania minimalne
Zasoby dyskowe	1. Macierz dyskowa musi być dostarczona z minimum: • 4 dyskami SAS 10k 2,5” o pojemności minimum 600GB • 29 dyskami NLSAS 3,5” o pojemności minimum 12TB 2. Macierz dyskowa musi mieć możliwość podłączenia dodatkowych dysków twardych o parametrach: • dyski SSD o pojemności minimum 3.2TB 3. Kontrolery macierzy dyskowej muszą obsługiwać minimum 250 dysków oraz pojemność surową minimum 2PB. Macierz musi mieć możliwość rozbudowy on-line do konfiguracji obsługującej minimum 500 dysków. 4. Należy dodatkowo dostarczyć dyski zapasowe lub pojemność zapasową w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 zapasowy dysk lub jego pojemność na 30 dysków danego typu. 5. Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpoczynać odtwarzanie danych na fizycznym dysku zapasowym lub pojemności zapasowej. 6. W przypadku stosowania dysku zapasowego, proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy).
Kontrolery macierzy dyskowej	1. Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (high availability cluster). Kontrolery muszą udostępniać dane poprzez iSCSI, FCP, CIFS oraz NFS. 2. Obszar pamięci cache przeznaczony do zapisów danych, musi posiadać lustrzaną kopię (ang. mirror). 3. W przypadku awarii zasilania, dane nie zapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub zachowane w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania. 4. Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze. 5. Macierz musi mieć minimum 128 GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. 6. System operacyjny kontrolerów musi natywnie obsługiwać automatyczny tiering bloków danych pomiędzy dyskami SSD, SAS, NL_SAS

	(macierz może alokować bloki dla danego wolumenu spośród wszystkich typów dysków: SSD, SAS, NL_SAS równocześnie). 7. Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie. Minimum RAID 1 (lub 10), 5, 6. Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone poziomami RAID 1 (lub 10), RAID 5, RAID 6 jednocześnie. 8. Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych. 9. Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256TB, plikowych o rozmiarze minimum 256TB. 10. Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.
Interfejsy	Macierz musi być wyposażona w następujące działające porty: • 4 porty 10GbaseT do podłączania hostów • 4 porty FC 16Gb do podłączania hostów – porty muszą być obsadzone odpowiednimi wkładkami SFP+ SR • 2 porty 1GbE Base-T do zdalnego zarządzania kontrolerem • 4 porty SAS minimum 12Gbs do podłączania półek dyskowych Porty przeznaczone do podłączenia hostów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami). Musi być możliwość rozbudowy on-line macierzy o minimum 16 portów (FC 16Gb lub 10Gb SFP+ lub 10GBaseT) jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów.
Kopie migawkowe	1. System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie Copy On Write dla dowolnego rodzaju danych (blokowe lub plikowe). Licencja na wszystkie opisane funkcjonalności musi obejmować całą powierzchnię użytkową macierzy. 2. Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika. 3. System operacyjny macierzy dyskowej musi umożliwiać wykonywanie kopii migawkowych wolumenów plikowych, w trybie on-line, bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen. 4. Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny. 5. Musi być możliwe zaprezentowanie kopii migawkowej w trybie do odczytu i zapisu.

Obsługiwane protokoły	1. System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i FCP - jeśli do uruchomienia potrzebna jest licencja, to Zamawiający wymaga uwzględnienie jej w cenie oferty oraz dostarczenia w ramach zawartej umowy. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz iSCSI - licencje na protokoły CIFS, NFS, FCP oraz iSCSI są przedmiotem obecnego postępowania. 2. Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, etc. firm trzecich.
Pozostałe wymagania	1. System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych: (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych. 2. Musi być możliwość konfiguracji macierzy dyskowej za pomocą GUI, zbieranie i wyświetlanie informacji o stanie zasobów macierzy dyskowej, prezentowanie i gromadzenie zdarzeń zachodzących w macierzy dyskowej oraz prezentowanie bieżących statystyk wydajnościowych macierzy dyskowej, podgląd parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym. 3. Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego. 4. W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft (MS Active Directory). 5. W celu zabezpieczania danych, macierz dyskowa musi mieć możliwość replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy i pracować w trybie asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gatawey, serwer pośredniczący, etc. Musi istnieć możliwość odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być zrealizowana zewnętrznym narzędziem software'owym. Licencja na replikację jest przedmiotem obecnego postępowania. 6. System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub analogicznych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu.
Gwarancja	Okres gwarancji producenta, jednak nie krótszy niż zadeklarowany w ofercie Wykonawcy. Serwis gwarancyjny realizowany w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia

	zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta/wykonawcy lub dedykowaną stronę www producenta/wykonawcy.
Wymiana dysków	Wymiana dysków musi być możliwa do dokonywania przez Zamawiającego.

4. Przełączniki LAN 10Gbps

4.1. Wymagania dotyczące przełączników

Parametr	Wymagania minimalne
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn. Możliwość montażu w szafie Rack dwóch przełączników obok siebie.
Porty	Minimum 12 portów 10GbE SFP+. Minimum 1 port USB
Wydajność	Obsługa minimum 4000 wirtualnych sieci. Przepustowość minimum 240 Gbps w trybie full-duplex, szybkość przełączania 178Mpps, wielkość tablicy MAC minimum 32000, rozmiar bufora pakietów minimum 1MB, 8 kolejek na port
Zgodność z protokołami	IEEE 802.1D Spanning Tree, ~~GARP i~~ GVRP IEEE 802.1p Traffic Prioritization IEEE 802.1Q VLAN Trunking IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1S Multiple Spanning Tree Protocol IEEE 802.1t IEEE802.1D maintenance ~~IEEE 802.1v VLAN Classification by Protocol & Port~~ IEEE 802.1x Port Based Network Access Control ~~IEEE 802.3 10 Mbps Ethernet~~ ~~IEEE 802.3I 10base -T~~ IEEE 802.3u 100Base-T Ethernet IEEE 802.3z 1000 Mbps Ethernet IEEE 802.3ab 1000Base-T IEEE 802.3ac Frame extension for VLAN tags IEEE 802.3ad Link Aggregation Control Protocol IEEE 802.3ae 10 Gig Ethernet ~~IEEE 802.2~~ IEEE 802.3x Flow Control ~~IEEE 802.3I~~ IEEE 802.1v VLAN Classification by Protocol & Port IEEE 802.1ab LLDP ANSI/TIA-1057-2006 LLDP-MEDW
Zarządzanie siecią i bezpieczeństwo	~~HTTP Over TLS~~ Radius Radius Accounting

	RADIUS Tunnel Authentication DHCP options ~~oraz BOOTP vendor extensions~~ Dynamic Host Configuration Protocol (DHCP) klient Bootstrap Protocol DNS Client Form-based File Upload in HTML ~~Simple Network Time Protocol (SNTP)~~ Wsparcie dla IPv6 IGMPv2 snooping MLD Snooping TLS protocol, version 1.0 PPP Extensible Authentication Protocol, EAP Hypertext Transfer Protocol -- HTTP/1.1 BSD Syslog Protocol IGMPv3 snooping SNMP v1 v2 ~~RMON~~ Simple Network Time Protocol (SNTP) Version 4 dla IPv4, IPv6 Port, VLAN mirroring DHCP Server Wsparcie dla ramek typu Jumbo 9,000 bajtów Broadcast storm control Możliwość wgrywania oprogramowania przez USB Zarządzanie za pomocą graficznej konsoli WEB Trivial File Transfer Protocol (TFTP) Rev. 2 Wsparcie dla agregacji LACP (802.3ad) - minimum 12 grup do 4 portów na grupę Honorowanie wartości 802.1p oraz IP DSCP Wsparcie kolejkowania Strict priority oraz algorytmu weighted round robin (WRR) wsparcie dla VLAN ID w ilości 4096 Private VLAN Guest VLAN Voice/Multicast TV VLAN ~~Locked Port~~ Dostępne profile konfiguracji portów
Warunki pracy	Wydajność pracy zasilaczy na poziomie min. 80% Temperatura pracy w zakresie od ~~0 do 50~~ 5 do 40 stopni Celsjusza Maksymalny pobór mocy ~~50W~~ 200W Wilgotność dla trybu pracy 85%
Certyfikaty i standardy	Zamawiający wymaga, aby oferowany przełącznik: - został wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 lub równoważnymi - posiadał deklarację CE

	- był zgodny z standardem RoHS
Gwarancja	~~Gwarancja na przełącznik typu "Lifetime" (tj. min. do 5 lat po tym, jak producent przestanie sprzedawać produkt wymieniony w matrycy End of Sale (EoS)).~~ Minimum ~~pięć lat~~ 3 lata gwarancji obejmującej naprawę lub wymianę sprzętu (przełącznik, zasilacz, wentylator, dostęp do nowych wersji oprogramowania) z czasem wysyłki sprzętu następnego dnia roboczego od przyjęcia zgłoszenia (możliwość zgłaszania awarii w trybie 24x7 poprzez ogólnopolską linię telefoniczną producenta).
Dodatkowe wyposażenie	Dla wskazanych 4szt. przełączników LAN wymagane jest wyposażenie ich łącznie w następujące wkładki/kable: 1) 18x SFP+, 10GbE, LR, 1310nm wavelength, up to 10km reach 2) 2x kabel SFP+ to SFP+, 10GbE, Copper Twinax Direct Attach Cable, 1m 3) 8x kabel SFP+ to SFP+, 10GbE, Copper Twinax Direct Attach Cable, 3m 4) 4x kabel SFP+ to SFP+, 10GbE, Copper Twinax Direct Attach Cable, 5m ~~5)~~ ~~4x kabel SFP, 1000BASE-T~~ 4x wkładka SFP 1000Base-T

5. System do wirtualizacji:

5.1. Wymagania dotyczące systemu wirtualizacji

System wirtualizacji musi spełniać co najmniej następujące wymagania:

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 576 logicznych wątków oraz do 12 TB 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 6 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).
13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003/R2, Windows Server 2008/R2, Windows Server 2012/R2, Windows Server 2016, Windows 7, Windows 8, Windows 8.1, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Solaris, Oracle Enterprise Linux, Debian GNU/Linux, CentOS, FreeBSD, Asianux, NeoKylin Linux, CoreOS, Ubuntu, 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. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
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. Mechanizm ten powinien być elementem składowym rozwiązania i nie powinien wymagać dodatkowej licencji na system operacyjny.
22. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.

23. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
24. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
25. 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.
26. 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 nieprzerwanie dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten ma umożliwiać zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.
27. 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.
28. 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.
29. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
30. Oprogramowanie musi być dostarczone wraz z minimum 2-letnią subskrypcją, rozpoczynającą się w dniu podpisania protokołu końcowego.
31. Licencja na oprogramowanie musi obejmować dowolną liczbę serwerów fizycznych (hostów), w których sumaryczna liczba fizycznych procesorów jest nie większa niż 12 CPU.
32. Oprogramowanie musi posiadać centralną konsolę graficzną do zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na wielu serwerach fizycznych:
    a. globalne zarządzanie kontrolą dostępu do serwerów i maszyn wirtualnych;
    b. wykonywanie automatycznych, bądź manualnych zadań w celu optymalizacji infrastruktury dla maszyn wirtualnych;
    c. widok całego systemu i zbioru maszyn wirtualnych (tzw. mapy Infrastruktury);
    d. możliwość monitorowania dostępności i wydajności maszyn wirtualnych;
    e. możliwość raportowania dostępności i wydajności maszyn wirtualnych;

f. funkcje ochrony dostępu zintegrowane z mechanizmem uwierzytelniania Windows;
g. planowanie zadań i ustawianie znaczników alarmów w celu generowania automatycznych powiadomień o statusie serwerów lub maszyn wirtualnych;
h. tworzenie obrazów maszyn wirtualnych;
i. klonowanie maszyn wirtualnych;
j. wykonywanie wielu kopii migawkowych (snapshot) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu zrobienia kopii.

6. System ochrony danych

6.1. Wymagania ogólne

1. Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu do zabezpieczania środowiska Data Center (baz danych, maszyn wirtualnych, serwerów wolnostojących).
2. Wymagane jest dostarczenie modułów oprogramowania:
   a. backupowego (aplikacja backupowa)
   b. umożliwiającego stworzenie systemu raportującego
   c. umożliwiającego zaindeksowanie oraz przeszukiwanie danych backupowych
   d. umożliwiającego stworzenie rozwiązania Continuous Data Protection (CDP) dla środowisk VMware
   e. umożliwiającego konfigurację/instalację deduplikatora
   f. umożliwiające zarządzanie oferowanym środowiskiem dedykowanym do zabezpieczania danych
   g. oferowane oprogramowanie powinno spełniać wszystkie wymienione w niniejszym rozdziale funkcjonalności. Wymagane wsparcie na oferowane oprogramowanie realizowane przez producenta w okresie min. 2 lat w trybie 9x5 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania.
3. Wymagane jest dostarczenie licencji w/w oprogramowania do zabezpieczania danych dla środowiska obejmującego zarówno serwery niezwirtualizowane oraz zwirtualizowane, charakteryzujące się sumaryczną ilością: 12 CPU. Zamawiający przewiduje w kolejnych latach rozbudowę zabezpieczanego środowiska, dlatego wymagana jest możliwość skalowania rozwiązania stworzonego w oparciu o licencje będące przedmiotem niniejszego zamówienia - poprzez dokładanie kolejnych licencji. Licencje, będące przedmiotem niniejszego zamówienia, powinny umożliwić skonfigurowanie deduplikatora o pojemności nie mniejszej niż 24TB netto oraz umożliwić zabezpieczenie dowolnej ilości maszyn wirtualnych (vSphere 6.5) w trybie CDP pracujących w środowisku liczącym 12 CPU.

6.2. 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.
2. 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.
3. W przypadku zabezpieczania baz danych i aplikacji, wymagana możliwość realizacji kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).
4. Zabezpieczane serwery muszą być backupowane bezpośrednio na dyski de-duplikatora (zainstalowanego/skonfigurowanego w oparciu o licencje będące przedmiotem niniejszego zamówienia) bez pośrednictwa jakichkolwiek innych urządzeń/serwerów. Dostarczone licencje (dotyczy aplikacji backup'owej oraz de-duplikatora) powinny umożliwiać całkowitą utylizację wymaganej przestrzeni de-duplikatora.
5. Transfer danych z zabezpieczanych serwerów do oferowanego de-duplikatora nie może się odbywać po sieci SAN.
6. Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej:
   a. backup pojedynczych plików
   b. backup całych systemów plików
   c. backup baz danych w trakcie ich normalnej pracy
   d. backup ustawień systemu operacyjnego Windows
   e. backup całych obrazów maszyn wirtualnych systemu VMware vSphere
   f. backup całych obrazów maszyn wirtualnych systemu Hyper-V
7. Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio ze zdalnych oddziałów do oferowanego de-duplikatora bez konieczności instalacji jakiegokolwiek sprzętu w oddziale. Powyższa funkcjonalność wymagana jest dla następujących typów danych:
   a. backup pojedynczych plików
   b. backup całych systemów plików
   c. backup baz danych w trakcie ich normalnej pracy
8. W przypadku zabezpieczania środowisk zdalnych, oferowane rozwiązanie backupowe nie może wymagać zaangażowania ze strony personelu w oddziale.
9. 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.

10. Oferowane rozwiązanie backupowe musi umożliwiać odtworzenie
    a. plików
    b. baz danych

    na docelową maszynę w oddziale - z poziomu centralnej konsoli systemu backupowego. Wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.
11. 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.
12. 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 de-duplikacji.

    Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.
13. 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.
14. Wymaga się, aby oprogramowanie backupowe przesyłało na oferowanego de-duplikatora tylko unikalne bloki, nie znajdujące się na tym urządzeniu, w efekcie skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.
15. Funkcjonalność de-duplikacji nie może wymagać instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.
16. 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.
17. Wymaga się, aby oprogramowanie backupowe realizowało wyłącznie - logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą być 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.
18. Wymagana możliwość definiowania w konsoli oprogramowania backupowego ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy muszą być automatycznie usunięte.

19. 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:
    a. Czas przechowywania backupów dziennych
    b. Czas przechowywania backupów tygodniowych
    c. Czas przechowywania backupów miesięcznych
    d. Czas przechowywania backupów rocznych
20. Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Wymagana możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:
    a. wybranych typów plików, np. dla plików z rozszerzeniem mp3
    b. dla całych katalogów (np.: c:\windows)
    c. dla pojedynczych plików
21. 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 powinien być przechowywany bezterminowo, a o jego usunięciu mógłby zdecydować jedynie administrator.
22. Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (minimum administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym.
23. Wymagana możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni przeznaczonej na składowanie de-duplikatów.
24. Bloki przesyłane z zabezpieczanych serwerów do oferowanego de-duplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.
25. Wymagana jest autentykacja komunikacji między klientem a serwerem backupu (farmą serwerów) oparta na certyfikatach.
26. Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, wymagane odtworzenie danych w jednym kroku.
27. Wymagana możliwość limitowania wielkości zadania backupowego, jeśli zadanie backupowe przekroczy zdefiniowaną wielkość, wówczas nie może być zapisane w systemie backupowym.
28. Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu, tak aby odpowiednia moc procesora pozostała do wykorzystania dla innych zadań.
29. Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0, 6.5.

    Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu:
    a. Backup całych maszyn wirtualnych

b. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk
c. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia, które wirtualne dyski VMware mają być backupowane
d. W trakcie backupu, odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware)
e. Wykonywanie backupu obrazów maszyn wirtualnych - VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk)
f. Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego, zgodnie z przytoczonymi wymaganiami dla de-duplikacji.
g. Powyższe metody backupu muszą być wbudowane w oferowany system backupu, nie powinny wymagać tworzenia skryptów/dodatkowych komend.

30. Oferowany system musi pozwalać na szybkie odtworzenie:
    a. całych obrazów maszyn wirtualnych
    b. pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej
31. Wymaga się, aby oferowane rozwiązanie backupowe umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami:
    a. odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane będą tylko te bloki wirtualnej maszyny/dysku, które uległy zmianie od ostatniego backupu
    b. odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane będą tylko te bloki wirtualnej maszyny/dysku, które uległy zmianie od ostatniego backupu
    c. 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
    d. możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows), zamiast odtwarzania backupów, zapewnienie możliwości 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.
32. 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.

33. 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.
34. 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:
    a. odtworzenie maszyny wirtualnej na zdefiniowanym Data Center/Data Store
    b. weryfikację podstawowych procesów
    c. możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej

    Wymagana dostępność informacji w konsoli systemu backupu o statusie (poprawna/niepoprawna) weryfikacji maszyny wirtualnej.
35. Administrator (właściciel) danej maszyny wirtualnej VMware vSphere musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy też administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
36. 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.
37. Oferowane rozwiązanie backupowe musi umożliwiać tworzenie automatycznych polityk backupowych dla:
    a. Folderu
    b. Resource Pool
    c. systemu VMware vSphere

    Wymagane jest, aby dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie Vmware, spowodowało automatyczne backupowanie dodanej maszyny wirtualnej, zgodnie z polityką zdefiniowaną dla folderu hosta czy resource pooli w systemie VMware.
38. 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.
39. 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.
40. Wymaga się, aby inicjowanie backupu oraz odtwarzanie maszyn wirtualnych VMware dostępne było z poziomu graficznego interfejsu, linii komend oraz przez REST API.

41. 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, w sposób opisany w punkcie b., powinno umożliwiać 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 (lit. a b, c) 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.
42. Oferowane oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V.
43. Wymagana możliwość odtworzenia danych:
    a. z zabezpieczanego serwera / komputera,
    b. z konsoli systemu backupowego.
44. Wymagana możliwość odtworzenia:
    a. pojedynczego pliku,
    b. zabezpieczanej bazy danych.
45. 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.
46. W przypadku odtwarzania danych poprzez interfejs dostępny na zabezpieczanym serwerze/laptopie wymagany mechanizm autentykacji użytkowników spełniający funkcjonalności:
    a. mechanizm wbudowany w system backupowy
    b. mechanizm zintegrowany z usługami katalogowymi
    c. w przypadku wykorzystania AD, użytkownicy będący w domenie nie powinni być zobligowani do ponownego logowania się do systemu backupu w przypadku konieczności
        i. odtworzenia danych
        ii. przeszukania zwartości swoich backupów
        iii. wykonania backupu

47. 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.
48. 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).
49. Wymaga się, aby oferowany system backupu posiadał możliwość bezpośredniego raportowania o błędach do serwisu producenta
50. 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.
51. Oferowany system backupu powinien posiadać możliwość automatycznej samoaktualizacji poprzez automatyczne ściąganie nowych wersji oprogramowania od producenta.
52. Oferowany system backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.

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

1. W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania zużycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów:
    a. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)
    b. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych)
    c. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów
    d. Zbiorcze zestawienie zabezpieczanych serwerów, które w sposób ciągły (kilka razy pod rząd) mają problem z backupami
    e. Zestawienie zabezpieczanych systemów plików, które w ogóle nie są backupowane
    f. Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii)
    g. Najmniej wiarygodne zabezpieczane serwery (procent nieudanych backupów)
    h. Lista najwolniejszych/najszybszych zabezpieczanych maszyn

i. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego
j. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu, do którego się dotwarzamy)
k. Liczba danych backupowanych dziennie
l. Liczba zadań backupowych dziennie
m. Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN)
n. Zużycie mediów backupowych i napędów taśmowych
o. Aktualna konfiguracja systemu backupowego
p. Historia zmian konfiguracji systemu backupowego
q. Posiadane licencje systemu backupowego
r. Wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center)

2. 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.

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

1. Integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT), vSphere Web Client GUI.
2. Wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion.
3. Możliwość integracji z VMware vRealize Operations Manager.
4. Rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi.
5. 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.
6. Możliwość tworzenia tzw. CONSISTENCY GROUP, zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM).
7. 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.
8. Wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającym odnotowanie wszystkich zmian zabezpieczanego środowiska.
9. Odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN.

10. Wbudowana funkcjonalność de-duplikacji oraz kompresji w przypadku transmisji danych poprzez WAN.
11. Wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. trzech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP).
12. Proponowane rozwiązanie powinno umożliwiać:
    a. stworzenie DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware vSphere,
    b. operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami ,
    c. MIGRACJĘ danych w trybie ON-LINE na inne zasoby dyskowe.
13. Równoległe wsparcie środowisk lokalnych oraz zdalnych - wymagana możliwość pracy w trzech 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.
14. Granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją.
15. Architektura FAULT-TOLERANT, brak pojedynczego punktu awarii.
16. Działanie rozwiązania będącego przedmiotem zamówienia nie może mieć negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji.
17. Wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund.
18. Proponowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa:
    a. RPO=30s z ostatnich 24h,
    b. RPO=24h z ostatniego tygodnia,
    c. RPO=1tydzień z ostatniego miesiąca.
19. Możliwość odtworzenia zabezpieczanego środowiska do DOWOLNEGO punktu w czasie .
20. Możliwość wyboru trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM).
21. Rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu.
22. Możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji.
23. Wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS.
24. 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.

25. Możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM).
26. Możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK.
27. Możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE).
28. Możliwość skryptowego tworzenia planów RECOVERY.

6.5. Wymagania funkcjonalne dotyczące de-duplikatora skonfigurowanego w oparciu o licencje będące przedmiotem zamówienia (wymagany rozmiar de-duplikatora został podany wcześniej)

1. Rozwiązanie, powstałe w wyniku instalacji/konfiguracji licencji będących przedmiotem zamówienia, musi być przeznaczone do de-duplikacji, dedykowane do przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszym rozdziale.
2. Oprogramowanie będące przedmiotem zamówienia musi umożliwiać konfigurację de-duplikatora na platformie VMware vSphere 6.5 oraz Microsoft Windows Server 2012 R2 z Hyper-V, o wcześniej określonej przestrzeni (powierzchni użytkowej dedykowanej do przechowywania de-duplikatów) bez uwzględniania mechanizmów protekcji. Wymagane skalowanie do min. 90TB powierzchni netto w ramach tego samego urządzenia.
3. De-duplikator musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami:
    a. CIFS,
    b. NFS,
    c. De-duplikacja na źródle (alternatywnie OST/BOOST/CATALYST),
    d. w obrębie oferowanej pojemności urządzenia.
4. Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia.
5. Urządzenie musi pozwalać na jednoczesną obsługę minimum 20 strumieni.
6. Oferowane urządzenie musi de-duplikować 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.
7. 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.
8. 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 de-duplikacji.

9. Niedopuszczalna jest de-duplikacja stałym blokiem o ustalonej tej samej długości, możliwość manualnej zmiany (bądź poprzez oskryptowanie) długości bloku de-duplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest każdy strumień danych.
10. Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, de-duplikacja 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.
11. Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji 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 de-duplikacji na źródle).
12. Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych.
13. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo skompresowane.
14. Oferowane rozwiązanie musi wspierać oferowaną aplikację backup'ową oraz co najmniej: VERITAS NetBackup, EMC Networker, Veeam, Oracle RMAN, Microsoft SQL Server Management Studio.
15. W przypadku współpracy z każdą z poniższych aplikacji:
    a. RMAN (dla ORACLE)
    b. Microsoft SQL Server Management Studio (dla Microsoft SQL)
    c. VERITAS NetBackup
    d. EMC NetWorker
    e. Veeam

    urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesyłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.
    De-duplikacja 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.
16. W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
17. 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%.

18. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia tego samego typu. Wymagane są następujące tryby pracy replikacji:
    a. jeden do jednego,
    b. wiele do jednego,
    c. jeden do wielu,
    d. 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 przedmiotowego zamówienia.
19. W przypadku wykorzystania portów Ethernet do replikacji, urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
20. W przypadku replikacji danych między dwoma urządzeniami, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:
    a. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących,
    b. replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu,
    c. 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.
21. Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
22. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
23. De-duplikator 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).

24. De-duplikator 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).
25. De-duplikator 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.
26. Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
27. Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego poprzez:
    a. CIFS,
    b. NFS,
    c. wymagany protokół umożliwiający de-duplikację na źródle.
28. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
29. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu), nie może wymagać definiowania BLACKOUT WINDOW czyli okna czasowego dedykowanego dla procesu czyszczenia, podczas którego nie są realizowane procesy backupu / odtwarzania danych czy replikacji.
30. Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
31. Wymagana możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
32. 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.
33. Urządzenie musi mieć możliwość zarządzania poprzez
    a. interfejs graficzny dostępny z przeglądarki internetowej,
    b. 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 zamówienia.
34. Możliwość uruchomienia zdalnych konsol dla:
    a. aplikacji backup'owej
    b. systemu dedykowanego do raportowania
    c. systemu dedykowanego do przeszukiwania danych backup'owych
    d. systemu CDP

e. de-duplikatorów

stworzonych w oparciu o oprogramowanie będące przedmiotem zamówienia, możliwość zdalnego uruchomienia oraz wyłączenia w/w komponentów.

35. Zapewnienie podglądu on-line takich elementów jak:
    a. aktywność procesów backup'owych,
    b. aktywność procesów replikacyjnych,
    c. aktualny status,
    d. alarmy,
    e. w przypadku zaoferowanej aplikacji backup'owej oraz de-duplikatora.
36. Możliwość zarządzania procesem wyszukiwania danych backup'owych.
37. Integracja z oferowanym rozwiązaniem dedykowanym do raportowania, możliwość inicjowania raportów.

7. Rozbudowa switch'a Aruba o 2 moduły

7.1. Wymagania

Rozbudowa posiadanego przez Zamawiającego przełącznika Aruba 5412R zl2 o dwa fabrycznie nowe moduły. Każdy z nich powinien być wyposażony w min. 8 portów 1/10Gigabit Ethernet SFP+, spełniających standardy komunikacyjne IEEE 802.3, IEEE 802.3ab, IEEE 802.3ae. Każdy z modułów musi być wyposażony w min. 2 wkładki działające w standardzie 10G SFP+ LC LR 10km SMF.

Moduły muszą być objęte dożywotnią (tak długo jak Zamawiający posiada produkt) gwarancją producenta, zapewniającą wysyłkę sprawnego sprzętu zamiennego – o takich samych lub równoważnych parametrach, na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego (pomocy technicznej, nie ograniczonej jedynie do zgłaszania awarii). Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

8. Wdrożenie i uruchomienie

8.1. Instalacja oferowanej macierzy dyskowej

1. Montaż macierzy dyskowej w szafie Rack.
2. Podłączenie macierzy do infrastruktury sieci LAN.
3. Podłączenie macierzy do infrastruktury sieci SAN.
4. Inicjalizacja macierzy dyskowej .
5. Aktualizacja oprogramowania układowego (firmware) do najnowszej, stabilnej, zalecanej przez producenta wersji.

6. Konfiguracja przestrzeni dyskowej (pule dyskowe, grupy RAID).
7. Konfiguracja zasobów dyskowych dedykowanych dla środowiska wirtualizacji z wykorzystaniem blokowych protokołów dostępu.
8. Konfiguracja przestrzeni dyskowych dedykowanych jako przestrzeń serwera plików dla użytkowników.
9. Konfiguracja uprawnień dostępu do danych blokowych.
10. Testy wydajności.
11. Optymalizacja wydajności.

8.2. Montaż oferowanych serwerów fizycznych

1. Montaż serwerów w szafie Rack.
2. Podłączenie serwerów do zasilania.
3. Aktualizacja mikrokodu (firmware) de-duplikatora do najnowszej zalecanej przez producenta wersji.
4. Podłączenie maszyn fizycznych do infrastruktury sieci LAN/SAN.

8.3. Konfiguracja sieci LAN/SAN

1. Montaż przełączników w szafie Rack.
2. Podłączenie do sieci LAN.
3. Zestawienie połączenia pomiędzy serwerownią Centrum Komiksu i Narracji Interaktywnej a serwerownią zlokalizowaną w budynku EC1 Wschód – za pomocą istniejącego okablowania. Połączenie ma być zestawione przy pomocy dostarczonych przełączników, objętych niniejszym zamówieniem oraz istniejących przełączników Aruba 5412R zl2.
4. Konfiguracja przełączników LAN/SAN.
5. Aktualizacja mikrokodu (firmware) przełączników do najnowszej zalecanej przez producenta wersji.
6. Podłączenie oferowanej macierzy do sieci LAN/SAN.
7. Podłączenie oferowanych serwerów do sieci LAN/SAN.
8. Definicja stref dostępu w sieci SAN, a w szczególności:
    a. Definicja aliasów dla sieci FC,
    b. Definicja stref dostępu dla sieci FC,
    c. Wirtualnych sieci LAN (VLAN) dla sieci iSCSI.

   Dla zapewnienia dostępu do danych macierzy dyskowych dla maszyn fizycznych.

8.4. Wirtualizacja środowiska serwerowego

1. Instalacja systemu wirtualizacji na oferowanych maszynach fizycznych.
2. Konfiguracja parametrów serwerów wirtualizacyjnych: adresacja IP, routing, DNS, synchronizacja czasu.
3. Rejestracja serwerów wirtualizacji serwerowej w macierzy dyskowej.
4. Prezentacja przestrzeni macierzy dyskowej dla serwerów wirtualizacyjnych.

5. Organizacja systemu plików na wydzielonych zasobach macierzy dyskowej dedykowanych do składowania plików maszyn wirtualnych.
6. Konfiguracja sieci wirtualnych dedykowanych dla maszyn wirtualnych oraz mechanizmów migracji maszyn wirtualnych pomiędzy maszynami fizycznymi, w trybie on-line.
7. Instalacja oprogramowania służącego do zarządzania środowiskiem wirtualizacji serwerowej oraz monitorowania i konfiguracji go.
8. Konfiguracja klastra wysokiej dostępności.
9. Konfiguracja mechanizmu migracji maszyn wirtualnych pomiędzy maszynami fizycznymi w trybie on-line.
10. Instalacja mechanizmu automatyzacji aktualizacji środowiska.
11. Aktualizacja środowiska wirtualnego do najnowszej stabilnej wersji.
12. Testy mechanizmów migracji maszyn wirtualnych pomiędzy maszynami fizycznymi.
13. Testy mechanizmów klastra wysokiej dostępności.

8.5. Implementacja systemu kopii zapasowych

1. Konfiguracja serwera fizycznego, dedykowanego do zadań serwera kopii zapasowych.
2. Podłączenie serwera do sieci LAN/SAN.
3. Konfiguracja serwera fizycznego:
    a. parametry dostępu do interfejsu zarządzania serwerem,
    b. konfiguracja lokalnej przestrzeni dyskowej.
4. Aktualizacja mikrokodu (firmware) komponentów serwera do najnowszej zalecanej przez producenta wersji.
5. Instalacja systemu operacyjnego wirtualizatora dla systemu kopiowania i odtwarzania danych.
6. Konfiguracja parametrów systemu 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 de-duplikacji danych jako maszyna wirtualna.
10. Konfiguracja parametrów sieciowych systemu de-duplikatora.
11. Konfiguracja protokołów dostępowych do de-duplikatora.
12. Konfiguracja urządzeń składowania danych (repozytoria kopii zapasowych):
    a. Przestrzenie dyskowe,
    b. Przestrzenie dyskowe z de-duplikacją.
13. Organizacja przestrzeni dyskowej na obecnie posiadanych oraz dostępnych zasobach macierzy dyskowych oraz dedykowanie tejże przestrzeni na potrzeby systemu kopii zapasowych.
14. Konfiguracja przestrzeni dyskowej dedykowanej dla składowania unikatowych bloków.

15. Prezentacja danych dla systemu kopiowania i odtwarzania danych.
16. Konfiguracja polityk ochrony dla wskazanych maszyn wirtualnych/fizycznych:
    a. Definicje typów kopii zapasowych (obraz maszyny, dane plikowe, dane aplikacyjne w trybie online, dane aplikacyjne w trybie offline),
    b. Definicja harmonogramów,
    c. Definicja miejsc składowania kopii zapasowych,
    d. Definicja polityk retencji,
    e. Testy odtwarzania danych.

9. Dokumentacja powdrożeniowa

Wykonanie dokumentacji powdrożeniowej do akceptacji Zamawiającego, zwierającej co najmniej:

1. Stworzoną architekturę;
2. Opis konfiguracji systemu – nie jest dopuszczalne użycie czystego „raportu konfiguracji" z wdrożonych aplikacji;
3. Opis wszystkich obiektów (polityk, urządzeń, harmonogramów) wraz z przyczyną utworzenia oraz zależnościami z innymi obiektami;
4. Opis procedur odtwarzania wykonanych w ramach wdrożenia dla przyszłych przypadków;
5. Opis procedur administracyjnych;
6. Zatrzymanie i uruchomienie całego systemu kopii zapasowych;
7. Procedura DR restore;
8. Opis możliwości przyszłej rozbudowy/modyfikacji systemu backup pod kątem dwóch lokalizacji.

10. Instruktaż administratorów

W ramach zamówienia, Wykonawca zobowiązany jest do przeprowadzenia instruktażu administratorów (minimum 4 osoby), w wymiarze 16 godzin (dwa dni robocze), w siedzibie Zamawiającego, w zakresie obsługi i konfiguracji dostarczonego systemu, a w szczególności:

1. Administracji systemem wirtualizacji,
2. Administracji systemem do tworzenia kopii zapasowych,
3. Przygotowania, utworzenia kopii zapasowej i jej odtworzenia.

11. Gwarancja oraz wsparcie techniczne

System musi być objęty serwisem gwarancyjnym producenta przez okres trwania umowy, polegającym co najmniej na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Przez naprawę rozumie się całkowite usunięcie usterki.