**INS/TI - 24/2024**

**Załącznik nr 1 do SWZ**

**Opis przedmiotu zamówienia / dane techniczne oferowanego sprzętu**

**Dane dotyczące Zamawiającego**

SIEĆ BADAWCZA ŁUKASIEWICZ - INSTYTUT NOWYCH SYNTEZ CHEMICZNYCH

Al. Tysiąclecia Państwa Polskiego 13A, 24 - 110 Puławy

**Dane dotyczące Wykonawcy**

Niniejsza oferta została złożona przez:

Ja / My, niżej podpisany/i

……………………………………………………………………………………………………………………………….

*Działając w imieniu i na rzecz:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **NAZWA WYKONAWCY/ÓW** | **ADRES/Y WYKONAWCY/ÓW** | **NIP, REGON, KRS WYKONAWCY/ÓW** |
|  |  |  | NIP:  REGON:  KRS: |

dotyczy postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez możliwości negocjacji (zgodnie z art. 275 pkt 1 pzp) na: **„Dostawa sprzętu i oprogramowania wraz z wdrożeniem kompleksowego systemu backupu”,** **Znak: INS/TI – 24/2024.**

Niniejszy załącznik stanowi jednocześnie szczegółowy opis przedmiotu zamówienia. Zaoferowany przez Wykonawcę sprzęt musi spełniać minimalne wymagania postawione w niniejszym załączniku w kolumnie „Minimalne wymagania Zamawiającego” oraz zostać dostarczony na warunkach określonych poniżej. Wykonawca w kolumnie „Dane techniczne oferowanego sprzętu/oprogramowania” winien odnieść się do każdego z wymagań minimalnych postawionych przez Zamawiającego w kolumnie „Minimalne wymagania Zamawiającego” wpisując TAK lub NIE. Wykonawca określa też producenta oraz model oferowanego sprzętu.

1. **Serwer – 1 szt.**

Producent oraz model oferowanego urządzenia: ……………………………

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** | **TAK /NIE** |
| **1.** | **Obligatoryjne wymagania Zamawiającego** |  |
| 1.1. | **Obudowa Rack** – o wysokości max. 2U umożliwiającą instalację min. 8 dysków 3,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |  |
| 1.2. | **Płyta główna** z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| 1.3. | **Chipset**  Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| 1.4. | **Procesor**  Zainstalowane dwa procesory min. ośmio-rdzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 134 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |  |
| 1.5. | **RAM**  Min. 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| 1.6. | **Zabezpieczenia pamięci RAM**  Advanced ECC, Memory Health Check, Memory Page Retire |  |
| 1.7. | **Gniazda PCIe**  - minimum 3 sloty PCIe x16 generacji min. 3 oraz 1 slot PCIe x4 generacji min. 3. |  |
| 1.8. | **Interfejsy sieciowe/FC/SAS**  Dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ nie zajmujące slotów PCIe.  Możliwość instalacji wymiennie modułów udostępniających:   * dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT * dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT * dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 * cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ * cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT * cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 * dwa interfejsy sieciowe 1Gb Ethernet   Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie Base-T. |  |
| 1.9. | **Dyski twarde**  Zainstalowane 2 x 960GB SSD vSAS SED, DWPD min. 1 oraz 6 x 4TB NearLine SAS  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.    Zainstalowane dwa dyski hot-plug M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. |  |
| 1.10. | **Kontroler RAID**  Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60. |  |
| 1.11. | **Wbudowane porty**  min. port USB 2.0 oraz port USB 3.0, port VGA. |  |
| 1.12. | **Video**  Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |  |
| 1.13. | **Wentylatory** Redundantne |  |
| 1.14. | **Zasilacze**  Min. dwa zasilacze Hot-Plug min. 700W Titanium |  |
| 1.15**.** | **Bezpieczeństwo** Zatrzask górnej pokrywy.  Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. |  |
| 1.16. | **Karta Zarządzania**  Niezależna karta 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 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, 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 serwerami fizycznymi, * Automatyczne zgłaszanie alertów do centrum serwisowego producenta * Automatyczne 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. * Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera |  |
| **1.17.** | **Oprogramowanie do zarządzania** Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * 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 * 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 oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji 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 i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| 1.18. | **Certyfikaty** Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklaracja CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022. |  |
| **2.** | **Gwarancja** |  |
| 2.1. | **Warunki gwarancji**  Zamawiający wymaga min. 36 miesięcy gwarancji producenta, możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365  następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej  (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***wykonawcy / producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. |  |
| 3. | **Dokumentacja** |  |
| 3.1. | **Dokumentacja użytkownika**  Zamawiający wymaga 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. |  |

1. **Serwer – 1 szt.**

Producent oraz model oferowanego urządzenia: ……………………………

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** | **TAK /NIE** |
| **1.** | **Obligatoryjne wymagania Zamawiającego** |  |
|  |  |  |
| 1.1. | **Obudowa -** Obudowa Rack o wysokości max. 2U umożliwiającą instalację min. 8 dysków 3,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |  |
| 1.2. | **Płyta główna -** Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| 1.3. | **Chipset** - Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| 1.4. | **Procesor** - Zainstalowane dwa procesory min. ośmio-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 134 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. Dla oferowanego serwera. |  |
| 1.5. | **RAM** Min. 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| 1.6. | **Zabezpieczenia pamięci RAM**  Advanced ECC, Memory Health Check, Memory Page Retire |  |
| 1.7. | **Gniazda PCIe**  - minimum 3 sloty PCIe x16 generacji min. 3 oraz 1 slot PCIe x4 generacji min. 3. |  |
| 1.8. | **Interfejsy sieciowe/FC/SAS**  **-** Dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ nie zajmujące slotów PCIe.  - Karta HBA posiadająca cztery zewnętrzne porty SAS.  Możliwość instalacji wymiennie modułów udostępniających:  - dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT  - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28  - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+  - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  - cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28  - dwa interfejsy sieciowe 1Gb Ethernet  Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie Base-T. |  |
| 1.9. | **Dyski twarde -** Zainstalowane 2 x 960GB SSD vSAS SED, DWPD min. 1 oraz 6 x 4TB NearLine SAS  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.    Zainstalowane dwa dyski hot-plug M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. |  |
| 1.10. | **Kontroler RAID** Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60. |  |
| 1.11. | **Wbudowane porty**  min. port USB 2.0 oraz port USB 3.0, port VGA. |  |
| 1.12. | **Video** Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |  |
| 1.13. | **Wentylatory** Redundantne |  |
| 1.14. | **Zasilacze** Min. dwa zasilacze Hot-Plug min. 700W Titanium |  |
| 1.15. | **Bezpieczeństwo** Zatrzask górnej pokrywy  Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. |  |
| 1.16. | **Karta Zarządzania**  Niezależna karta od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * szyfrowane połączenie (TLS) 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, 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 serwerami fizycznymi, * Automatyczne zgłaszanie alertów do centrum serwisowego producenta * Automatyczne 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. * Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera |  |
| 1.17. | **Oprogramowanie do zarządzania** Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * 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 * 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 oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji 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 i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| 1.18. | **Certyfikaty** Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklaracja CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022. |  |
| **2.** | **Gwarancja** |  |
| 2.1. | **Warunki gwarancji**  Zamawiający wymaga min. 36 miesięcy gwarancji producenta, możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365  następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej  (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***wykonawcy / producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. |  |
| **3.** | **Dokumentacja** |  |
| 3.1. | **Dokumentacja użytkownika**  Zamawiający wymaga 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. |  |

1. **Oprogramowanie do backupu**

**Opis wymogów funkcjonalnych dla systemu zarządzania danymi obejmujący backup serwerów fizycznych, aplikacji oraz maszyn wirtualnych.**

Uwaga:

Pojęcie **system** wskazuje na rozwiązanie zabezpieczające dane stanowiące jedno, spójne rozwiązanie, zarządzane z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie nie całkowicie niezintegrowanych pomiędzy sobą wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji.

Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych i pocztowych do archiwum (repozytorium dyskowe) po skopiowaniu tych zasobów system musi tworzyć skróty oraz kasować zarchiwizowane dane w pełni automatycznie. Obie funkcjonalności: kasowanie danych i tworzenie skrótów musi być dostępne co najmniej dla archiwizowanych danych plikowych z systemów Windows i Linux, oraz maili z systemów Exchange Onpremis i Exchange Online.

Jeśli przy danym punkcie wymogu występuje informacja „jako opcja” oznacza to iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność.

W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik będzie negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** | **Spełnia/nie spełnia** |
| 1. | Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych. |  |
| **2.** | Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia. |  |
| **3.** | Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizycznym (minimum 2xCPU po 16 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V. |  |
| **4.** | Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z częstotliwością replikacji bazy katalogowej nie dłuższym niż 15 minut (RPO nie większe niż 15 min dla uruchomienia zapasowego serwera zarządzającego). Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza to lokalizacja produkcyjna a druga i trzecia typu „standby” dla serwera zarządzającego. |  |
| **5.** | Jako opcja musi istnieć możliwość zainstalowania serwera zarządzającego na systemie operacyjnym Linux z zachowaniem możliwości replikacji bazy katalogowej i tworzeniem serwerów typu standby. |  |
| **6.** | Proces przełączenia serwera zarządzającego musi umożliwiać:   * Przełączenie automatyczne inicjalizowane przez administratora * Przełączenie automatyczne (bezobsługowe) w przypadku wykrycia awarii (w przypadku awarii serwera zarządzającego system automatycznie wykrywa awarie i przełącza działanie systemu na serwer zapasowy – standby, bez jakiejkolwiek interwencji administratora) |  |
| **7.** | Przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy różnymi typami infrastruktury:   * serwer fizyczny -> serwer fizyczny * serwer fizyczny -> serwer wirtualny (onpremis) * serwer fizyczny -> serwer wirtualny (AWS, Azure, Google) * serwer wirtualny (onpremis) -> serwer fizyczny * serwer wirtualny (onpremis) -> serwer wirtualny (onpremis) * serwer wirtualny (onpremis) -> serwer wirtualny (AWS, Azure, Google) |  |
| **8.** | Mechanizm przełączania serwera zarządzającego musi pozwalać (minimum) na wybór trybu:   * Test failover (testowanie mechanizmu przełączania) * Failover (produkcyjne przełączenie działania na serwer standby) * Maintenance failover (przełączenie w celu np. aktualizacji oprogramowania) |  |
| **9.** | Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji. |  |
| **10.** | Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich |  |
| **11.** | System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów. |  |
| **12.** | System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania i musi pozwalać na wyczyszczenie przestrzeni dyskowych (zamazanie) tak aby narzędziami niskiego poziomu nie było możliwości odzyskania tych danych. |  |
| **13.** | Administrator systemu musi mieć możliwość wybrania (minimum) plików z danej kopii backupowej i ich skasowania, tak aby nie było możliwości ich późniejszego odtworzenia z tej kopii. |  |
| **14.** | Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie |  |
| **15.** | System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu |  |
| **16.** | System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej |  |
| **17.** | Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji ze środowisk typu DMZ |  |
| **18.** | Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP |  |
| **19.** | System musi umożliwiać nie tylko szyfrowanie danych (kopii backupowych) ale także całej komunikacji pomiędzy komponentami systemu (minimum pomiędzy agentem backupowym a serwerem składującym i zarządzającym kopiami). |  |
| **20.** | System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interfejsu musi odbywać się co najmniej poprzez nazwę domeny, podsieć, zakres IP |  |
| **21.** | System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN |  |
| **22.** | System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia). |  |
| **23.** | Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh |  |
| **24.** | Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej |  |
| **25.** | Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych. |  |
| **26.** | Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB. |  |
| **27.** | System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji. |  |
| **28.** | System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu. |  |
| **29.** | Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej. |  |
| **30.** | System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości backupu z deduplikacją i odtwarzania wcześniejszych kopii danych |  |
| **31.** | System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie korzysta z bazy deduplikacyjnej. |  |
| **32.** | Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu. |  |
| **33.** | System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną |  |
| **34.** | System musi być odporny na tzw. „atak na wzorzec czasu”: to znaczy iż przy radykalnej zmianie czasu na serwerze zarządzającym System musi automatycznie zatrzymać co najmniej proces kasowania (ekspiracji) kopii backupowych generując odpowiednie alerty do czasu potwierdzenia tej zmiany przez administratora. |  |
| **35.** | System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD. |  |
| **36.** | System musi pozwalać na zarządzanie poprzez „cmd” z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH. |  |
| **37.** | Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach |  |
| **38.** | System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych) |  |
| **39.** | System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail |  |
| **40.** | Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu. |  |
| **41.** | Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem |  |
| **42.** | System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO |  |
| **43.** | System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password |  |
| **44.** | System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrujących zgodnymi z KMIP – minimum dla:   * + AWS CloudHSM   + Fortanix Data Security Manager   + HashiCorp Vault   + IBM Security Key Lifecycle Manager (SKLM)   + Safenet   + StorMagic SvKMS   + Thales CipherTrust Manager   + Vormetric   + Amazon Web Services (AWS) key management service   + Microsoft Azure Key Vault |  |
| **45.** | System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy |  |
| **46.** | System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:   * + Monitorowanie nietypowych zachować systemu backupowego obejmującego obszary:     1. Czyszczenia bazy deduplikacyjnej (DDB)     2. Zdarzeń w Systemie (events)     3. Ilości nieudanych zadań     4. Ilości zadań czekających     5. Ilości zadań zakończonych sukcesem     6. Konsoli monitorującej zadania     7. Czasu trwania zadań   + Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane   + Monitorowanie nietypowych aktywności na serwerach plikowych   + Monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików)   + Monitorowanie możliwego zagrożenia dotyczącego zaszyfrowania plików na serwerach   + Monitorowanie różnych typów plików i weryfikowanie czy typ pliku jest zgodny i czytelny z nagłówkiem tego pliku (detekcja uszkodzeń plików czy ich zaszyfrowania)   + Monitorowanie klientów Systemu i alertowanie o tych którzy tracą komunikację z Systemem   + Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem.   + Możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym   + Możliwość definiowania kierunki inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego   + Możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach |  |
| **47.** | Analiza zagrożeń (Threat Analysis) (jako opcja(, która skanuje pliki kopii zapasowych pod kątem infekcji złośliwym oprogramowaniem za pomocą wbudowanego mechanizmu skanowania opartego na sygnaturach. |  |
| **48.** | Analiza zbackupowanych danych plikowych (jako opcja) polegająca na umożliwieniu użytkownikom sprawdzenie zawartości kopii zapasowej w celu zidentyfikowania, czy są jakieś pliki zaszyfrowane, uszkodzone lub zmodyfikowane w nietypowy sposób za pomocą algorytmów entropijnych |  |
| **49.** | System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email. |  |
| **50.** | System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez:   * + Syslog serwer   + Splunk (dedykowany plug-in do Spluk dla analizy danych) |  |
| **51.** | Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach |  |
| **52.** | System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:   * Raport zmian/wzrostu środowiska systemu * Raport wykorzystania licencji * Raport wykonanych zadań backupowych * Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM |  |
| **53.** | System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail |  |
| **54.** | System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV |  |
| **55.** | System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryterii:   * Czas zadania dłuższy niż zadany * Ilość danych większa niż …. * Ilość danych mniejsza niż …. * Ilość nie zbackupowanych plików większa niż * Ilośc nie zbackupowanych plików większa niż …% * Wielkośc backupowanych danych wieksza niż … |  |
| **56.** | Notyfikacje alertów muszą być wysyłane minimum poprzez mail. |  |
| **57.** | Raport spełnienia wymogów SLA dla parametrów:   * + Ilości dodatkowych kopii backupowych   + RTO   + RPO |  |
| **58.** | System musi zapewniać funkcjonalność wznawiania zadań backupowych. |  |
| **59.** | System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych. |  |
| **60.** | System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy |  |
| **61.** | Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu |  |
| **62.** | System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków |  |
| **63.** | Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego. |  |
| **64.** | System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych. |  |
| **65.** | System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji. |  |
| **66.** | System ma realizować procesy backupu oraz odzyskiwania danych, procesy te muszą być uruchamiane ręcznie i poprzez wbudowany kalendarz, możliwość definiowania zadań poprzez wbudowany w system kalendarz musi być możliwa nie tylko dla zadań backupowych ale także dla zadań odtwarzania danych a więc restore |  |
| **67.** | System musi dla backupu środowiska AWS oferować:   * + Bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików   + Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.   + Możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej EC2   + Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją   + Możliwość wykonywania jednoprzebiegowego konsystentnego backupu maszyn wirtualnych EC2, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory   + Backup i odtwarzanie danych z baz danych RDS: MS SQL, MySQL, PostgreSQL oraz Oracle (eksport danych na storage backupowy)   + Możliwość wykonywania snapshotów baz danych AWS RDS: Aurora, MariaDB, Microsoft SQL Server, MySQL, PostgreSQL.   + Backup oraz odtwarzanie danych składowanych w usłudze S3, EFS oraz FSx.   + Możliwość zapisu danych zdeduplikowanych bezpośrednio w usłudze S3, bez konieczności używania dodatkowego cache’u oraz rozwiązan typu appliance   + Możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych EC2, na których zainstalowano oprogramowanie serwera backupowego   + Możliwość konwersji maszyn wirtualnych Microsoft Hyper-V, Vmware oraz Azure do maszyn wirtualnych EC2   + Możliwość konwersji maszyn wirtualnych EC2 do maszyn typu Vmware oraz Azure   + Możliwość wykonywania backupu usługi AWS DynamoDB   + Możliwość backupu środowiska VMWare Cloud on AWS   + Możliwość automatycznego wyłączania i włączania serwerów backupowych   + Możliwość automatycznej replikacji maszyn wirtualnych Vmware do AWS EC2   + Możliwość wykorzystania EBS Direct Read API w czasie backupu maszyn wirtualnych EC2   + Możliwość integracji z AWS KMS w celu zarządzania kluczami szyfrującymi   + Możliwość backupu maszyn wirtualnych EC2 z innego konta Amazon (Cross-account backup)   + Możliwość migracji zdeduplikowanych danych do chmury AWS za pomocą urządzenia Snowball   + Możliwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP HANA, Microsoft SQL Server, DB2, MongoDB, MySQL, PostgreSQL oraz pliki na systemach Windows oraz Linux |  |
| **68.** | System musi dla backupu środowiska Azure oferować:   * + Bezagentowy backup całych maszyn wirtualnych Azure VM i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików.   + Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.   + Możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej w Azure VM   + Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją   + Możliwość wykonywania jednoprzebiegowego konsystentnego backupu maszyn wirtualnych Azure VM, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory?   + Backup i odtwarzanie danych z baz danych (PaaS): MS SQL, MySQL, PostgreSQL (eksport danych na storage backupowy)   + Backup oraz odtwarzanie danych składowanych w Azure Blob oraz Azure File Shares oraz Azure Data Lake Storage Gen2   + Możliwość zapisu danych zdeduplikowanych bezpośrednio na Azure Blob Storage, bez konieczności używania dodatkowego cache’u oraz rozwiązan typu appliance   + Możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych Azure, na których zainstalowano oprogramowanie serwera backupowego   + Możlwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP for Oracle, SAP HANA, Microsoft SQL Server, DB2 oraz pliki na systemach Windows oraz Linux   + Możliwość migracji zdeduplikowanych danych do chmury Azure za pomocą Azure Data Box   + Możliwość automatycznego wyłączania i włączania serwerów backupowych   + Możliwość integracji z Azure Key Vault w celu zarządzania kluczami szyfrującymi   + Możliwość automatycznej replikacji maszyn wirtualnych Hyper-V i Vmware do Azure   + Możliwość automatycznej replikacji maszyn wirtualnych Azure pomiędzy regionami   + Możliwość backupu bazy danych Cosmos DB (Core SQL API)   + Możliwość konwersji backupu systemu operacyjnego Windows wraz z danymi do maszyny wirtualnej Azure   + Możliwość backupu Azure DevOps and GitHub |  |
| **69.** | System musi dla backupu środowiska GCP oferować   * + Bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików   + Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.   + Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją   + Backup i odtwarzanie danych z baz danych Cloud SQL: MySQL oraz PostgreSQL (eksport danych na dowolny storage backupowy)   + Backup oraz odtwarzanie danych składowanych w usłudze GCP Cloud Storage   + Możliwość zapisu danych zdeduplikowanych bezpośrednio w usłudze GCP Cloud Storage, bez konieczności używania dodatkowego cache’u oraz rozwiązan typu appliance |  |
| **70.** | System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie. |  |
| **71.** | System musi realizować funkcjonalność weryfikacji wykonanych kopii. |  |
| **72.** | System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:   * + Windows   + Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu |  |
| **73.** | System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, Tintri z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji. |  |
| **74.** | Dla producentów: NetApp, EMC i HDS system musi umożliwiać nie tylko integrację z mechanizmami tworzenia kopii migawkowych (tzw. Snapshot) ale musi integrować się także z mechanizmami replikacyjnymi, a więc sterować replikami wykonywanymi przez macierze |  |
| **75.** | System powinien umożliwiać składowanie kopii backupowych na storage obiektowym w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane |  |
| **76.** | System musi umożliwiać backup danych z zasobów obiektowych czy to chmurowych (minimum: AWS, Azure, Google, OCI czy onpremis (minimum: Red Hat Ceph Storage, Pure Storage FlashBlade) |  |
| **77.** | System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows |  |
| **78.** | System musi pozwalać na odtwarzanie tylko samych uprawnień do plików |  |
| **79.** | System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) |  |
| **80.** | System (jako opcja) powinien umożliwiać analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryterii powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log. |  |
| **81.** | Możliwość (jako opcja) odtwarzania backupów plikowych poprzez udostepnienia CIFS lub NFS. A więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS |  |
| **82.** | System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows |  |
| **83.** | System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix |  |
| **84.** | System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Oracle Linux, Linux, Ubuntu, |  |
| **85.** | System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris |  |
| **86.** | System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane. |  |
| **87.** | System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:   * Alibaba Cloud * Amazon * Google Cloud Platform * Huawei FusionCompute * Microsoft Azure * Microsoft Azure Stack Hub * Microsoft Azure Stack HCI * Microsoft Hyper-V * Kubernetes * Nutanix Acropolis Hypervisor (AHV) * OpenStack * Oracle Cloud Classic * Oracle Cloud Infrastructure * Oracle VM * Red Hat OpenShift * Red Hat Virtualization * vCloud Director * VMware   To znaczy musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granualnego odtwarzania pojedynczych plików. Dla maszyn wirtualnych musi być możliwość zainstalowania agenta plikowego i bazodanowego dla zabezpieczenia zasobów z wewnątrz maszyny wirtualnej – funkcjonalność ta musi być zawarta dla wszystkich wymaganach wirtualizatorów i być w cenie rozwiązania. |  |
| **88.** | System musi wspierać wersje środowiska VMware 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7, 7.0,7.0.3, 8.0 poprzez integrację z vStorage API |  |
| **89.** | Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS |  |
| **90.** | System musi wspierać środowisko Hyper-V dla:   * Microsoft Windows Server 2012 * Microsoft Hyper-V Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Hyper-V Server 2012 R2 * Microsoft Windows Server 2016 (z Core Edition) * Microsoft Hyper-V Server 2016 (z Core Edition) * Microsoft Windows Server, version 1709 (z Core Edition) * Microsoft Hyper-V Server, version 1709 (z Core Edition) * Microsoft Windows Server 2019 (z Core Edition) * Microsoft Hyper-V Server 2019 (z Core Edition) * Microsoft Windows Server 2022 (z Core Edition) * Microsoft Hyper-V Server 2022 (z Core Edition) |  |
| **91.** | System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych. |  |
| **92.** | System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V. |  |
| **93.** | System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:   * + Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure   + Hyper-V do: Azure, Amazon, Vmware   + Amazon do: Azure, Vmware   + Azure do: Amazon, Hyper-V, Vmware |  |
| **94.** | System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V |  |
| **95.** | System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:   * + Hyper-V   + Vmware |  |
| **96.** | Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure |  |
| **97.** | System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, Oracle, Informix na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik. |  |
| **98.** | System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, DB2, Informix konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny. |  |
| **99.** | Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów. |  |
| **100.** | Dla silników bazodanowych MS SQL, Oracle i SAP HANA musi istnieć mechanizm backupu logów transakcyjnych z częstotliwością co 1 minuta nawet w przypadku gdy serwer zarządzający systemem backupowym jest niedostępny |  |
| **101.** | Konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interfejs graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie |  |
| **102.** | System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników |  |
| **103.** | System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziału systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange |  |
| **104.** | System musi umożliwiać wykonanie kopii na gorąco aplikacji MS Exchange a następnie odzyskania pojedynczych wiadomości. Dedykowany agent do backupu Exchange musi wspierać backup środowiska Exchange DAG poprzez nazwę DAG nawet w konfiguracji bez adresu IP |  |
| **105.** | System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL |  |
| **106.** | Dla minimum mySQL i PostgresSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego |  |
| **107.** | Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle |  |
| **108.** | Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio |  |
| **109.** | Wsparcie dla backupu online dla minimum MS SQL Server 2005/2008/2008 R2/2012/2014/2016/2017/2019/2022 na platformie Windows |  |
| **110.** | Dedykowany agent bazodanowy dla backupu MS SQL (2017/2019/2022) na platformie Linux: Ubuntu, SuSe, RHEL |  |
| **111.** | Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore) |  |
| **112.** | Dedykowani agenci do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk, MongoDB |  |
| **113.** | Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, mySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów |  |
| **114.** | Możliwość backupu i odtwarzania (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365 z:   * + SharePoint Online   + Exchange Online   + OneDrive   + Teams |  |
| **115.** | Możliwość (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści (eDiscovery i Compliance Search) z danych backupowanych ze:   * + Skrzynek pocztowych (Exchange onpremis)   + Skrzynek journalingowych (Exchange onpremis)   + Ruchu pocztowego SMTP   + Exchange Online   + Serwerów plikowych   + Laptopów i desktopów   + OneDrive for Business   + SharePoint Online |  |
| **116.** | Możliwość backupu (jako opcja) danych z aplikacji Salesforce, minimalny zakres backupowanych danych to:   * + Standard objects   + Custom objects   + Dokumenty   + Załączniki   + CRM content   + Pliki |  |
| **117.** | System musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:   * Portal samoobsługowy musi być dostępny poprzez dowolną przeglądarkę sieci Internet minimum: Edge, Chrome, Opera, Mozilla, Safari * System musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh * Dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android * Dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa. * System musi zapewniać współdzielenie plików pochodzących z backupu laptopów i destopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny. * Każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to: * Odtwarzanie własnych danych * Uruchomienie backupu * Wstrzymanie backupu * Możliwość zdefiniowania innego okna backupowego * Możliwość monitorowania postępu działania zadania * Możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN) * Zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane * Możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub) |  |
| **118.** | Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych. |  |
| **119.** | System musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa) takie jak:   * Oprogramowanie musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych. * Oprogramowanie musi być zintegrowane z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych. * Oprogramowanie musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych. Oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej. * Oprogramowanie musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów |  |
| **120.** | System musi (jako opcja) umożliwiać rozbudowę o archiwizację poczty (minimum Exchange), archiwizacja poczty musi umożliwiać archiwizowanie maili ze skrzynek pocztowych oraz archiwizowanie ruchu pocztowego (journaling lub SMTP journaling) |  |
| **121.** | System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok….) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie |  |
| **122.** | System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Unix i Linux. |  |
| **123.** | System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym |  |
| **124.** | System (jako opcja) musi posiadać zaawansowaną funkcjonalność analizy zasobów plikowych minimum o funkcjonalnościach:   * + Detekcja powtarzających się zasobów   + Raportowanie praw dostępu do plików   + Raportowanie i analiza dostępu do zasobów i ich modyfikacji   + Możliwość kasowania plików z zasobów produkcyjnych |  |
| **125.** | System (jako opcja) musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych ale i z kopii backupowej |  |
| **126.** | Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell |  |
| **127.** | Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy |  |
| **128.** | Agent do backupu systemów plikowych: Lustre, GlusterFS |  |
| **129.** | Wsparcie (jako opcja) dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VIAO (VSphere APIs for I/O |  |
| **130.** | System musi zawierać moduł do monitorowania i zarządzania taśmami wynoszonymi z bibliotek taśmowych o funkcjonalnościami minimum:   * + Identyfikacja taśm, które muszą być wyciągnięte z biblioteki   + Identyfikacja taśm, które można z powrotem wstawić do biblioteki taśmowej   + Automatyczne przenoszenie taśm w bibliotece i notyfikacja administratorów   + Identyfikacja i monitorowanie nośników (taśm) w trakcie transportu |  |
| **131.** | Możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy |  |
| **132.** | Możliwość (jako opcja) rozbudowy środowiska o moduł VTL dla backupu danych po sieci SAN i LAN na dowolnym sprzęcie typu x86 |  |
| **133.** | Możliwość włączenia backupu pojedynczego pliku wieloma strumieniami |  |
| **134.** | Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk |  |
| **135.** | Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych |  |
| **136.** | Dedykowane moduły do integracji z Terraform |  |
| **137.** | Możliwość anonimizacji danych wrażliwych (data masking) minimum dla logów systemu wysyłanych np. do wsparcia |  |
| **138.** | Podstawowe komponenty systemu jak: serwer zarządzający, serwery składujące i deduplikujące dane muszą wspierać system operacyjny Linux, a więc musi istnieć możliwość bezpośredniego zainstalowania na systemie Linux tych komponentów bez jakiejkolwiek warstwy wirtualizacyjnej |  |
| **Wymogi dla licencjonowania (licencjonowanie typu perpertual)** | |  |
| **1.** | Niedopuszczalne jest aby licencjonowanie było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL…) czy to z deduplikacją czy bez. |  |
| **2.** | Niedopuszczalne jest aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych. |  |
| **3.** | Niedopuszczalne jest aby licencjonowanie zależne było od ilości serwerów fizycznych czy ich mocy (ilości procesorów) niezależnie czy dane są z nich backupowane bezpośrednio czy tworzą platformę wirtualizacyjną, która jest backupowana. |  |
| **4.** | Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu |  |
| **5.** | Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:   * + nielimitowaną ilość bibliotek taśmowych i napędów fizycznych   + nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google) |  |
| **6.** | W przypadku wielu lokalizacji licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami |  |
| **7.** | Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych |  |
| **8.** | Do dostarczonych licencji jest wymagane 12 miesięczne wparcie producenta lub autoryzowanego partnera serwisowego (pierwsza i druga linia wsparcia świadczona w języku polskim lub angielskim) zapewniające wsparcie techniczne w trybie 12/5 oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. W przypadku serwisu świadczonego przez autoryzowanego partnera serwisowego producenta na terenie Polski wymagane jest potwierdzenie jakości świadczonych usług poprzez certyfikat ISO 9001:2015 na świadczone usługi serwisowe. |  |
| **9.** | Zaoferowane licencje na system muszą zapewnić backup danych ze środowiska o wielkości minimum 20 maszyn wirtualnych |  |

1. **Macierz pamięci dyskowej**

Producent oraz model oferowanego urządzenia: ……………………………

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** | **TAK / NIE** |
|  | **Obligatoryjne wymagania Zamawiającego** |  |
| **1.** | **Macierz** Obudowa RACK 2U powinna pozwalać na zamontowanie 24 dysków 2.5"  Macierz powinna posiadać dwa redundantne kontrolery.  W każdym z kontrolerów powinno być dostępne po 16GB pamięć cache (zapisu) mirrorowanej między kontrolerami, zabezpieczonej na wypadek awarii prądu przez min. 72h.  W każdym z kontrolerów powinno być dostępne cztery porty 12GB SAS (należy dołączyć odpowiednie sześć kabli do podłączenia serwerów o długości co najmniej 2m przeznaczonych przez producenta do pracy z tym urządzeniem). |  |
| **2.** | **Dyski:** W macierzy powinno być zainstalowane co najmniej szesnaście dysków SSD SAS o pojemności co najmniej 1.92TB i wydajności 24Gbps a wraz z nią dostarczony minimum 1 identyczny dysk dodatkowy w oryginalnym opakowaniu producenta.  Macierz ma mieć możliwość rozbudowy do co najmniej 8PB z użyciem zainstalowanych kontrolerów. |  |
| **3.** | **Funkcjonalności:** Macierz musi posiadać możliwość obsługi standardowych poziomów RAID - 0, 1, 5, 6, 10 lub parzystości opartej na przestrzeniach dyskowych w ramach tego samego rozwiązania - wybór podczas konfiguracji  Wsparcie dla autotieringu do trzech tierów musi wspierać thin provisioning i snapshoty w standardzie redirect on write szyfrowanie dysków |  |
| **4.** | **Zarządzanie:** Macierz musi dawać możliwość zarządzania zarówno z interfejsu graficznego obsługującego HTML5 jak i CLI.  Obsługa z aplikacji opartej na technologii JAVA jest wykluczona  Powiadamianie mailem o awarii, umożliwiające maskowanie mapowania dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN”ów oraz 1024 kopii migawkowych na całą macierz.  Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.  Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering).  Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków.  Musi istnieć możliwość wykorzystania dysków SSD jako cache macierzy oraz możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.  Macierz musi mieć możliwość obsługi CLI API, Redfish/Swordfish REST API |  |
| **5.** | **Replikacja:** W przypadku macierzy FC lub iSCSI macierz musi mieć możliwość asynchronicznej replikacji danych do drugiej takiej samej macierzy w innej lokalizacji  Do uruchomienia tej funkcjonalności nie powinno być potrzeby użycia licencji z poza oferty  Macierz musi posiadać wsparcie dla oprogramowania:   * *VMware Site Recovery Manager* * *VMware vSphere (ESXi) vCenter* * *VMware Site Recovery Manager* * *Microsoft Hyper-V* * *Wsparcie dla systemów* * *Windows 2022, 2019 and 2016* * *RHEL 8.2 and 7.8* * *SLES 15.2 and 12.5* * *VMware 7.0 and 6.7* * *Citrix XenServer 8.x and 7.x* |  |
| **6.** | **Certyfikaty:** Urządzenie musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  Urządzenie musi posiadać deklarację CE. |  |
| **7.** | **Warunki gwarancji:**   1. Dostarczony sprzęt musi posiadać 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia - zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7. 2. Gwarancja musi obejmować całość rozwiązania - nie powinno być tak aby jakaś część tego rozwiązania nie podlegała gwarancji. 3. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. 4. Producent musi dawać możliwość rozszerzenia gwarancji do 7 lat 5. W przypadku konieczności naprawy lub wymiany dysku uszkodzony dysk pozostaje u zamawiającego. 6. Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka. 7. Powinna być możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. messenger, teams, WhatsApp. 8. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. 9. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji. 10. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. 11. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 12. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 13. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. |  |

1. **Wdrożenie systemu backupu**

Usługa polegająca na wdrożeniu proponowanego rozwiązania w siedzibie Zamawiającego opierać się będzie minimum na:

* instalacji fizycznej serwerów backup’owych w miejscu wskazanym przez Zamawiającego (lokalizacja A i lokalizacja B)
* inicjalizacji urządzeń, instalacji i aktualizacji oprogramowania i firmware’u
* instalacji oprogramowania backupowego w maszynie wirtualnej Windows na serwerach w lokalizacjach A i B
* zaprojektowaniu i wdrożeniu polityk backupu, według zaleceń i po konsultacjach z Zamawiającym i z uwzględnieniem środowiska Zamawiającego
* skonfigurowaniu repliki backup’u do lokalizacji B
* testów odtworzeniowych
* szkoleniu z obsługi oprogramowania backup’owego (min.12h w kilku terminach uzgodnionych z Zamawiającym)
* przygotowaniu i przekazaniu Zamawiającemu dokumentacji powykonawczej

1. **Oprogramowanie systemowe**

Ze względu na posiadane już oprogramowanie i istniejącą infrastrukturę Zamawiającego oraz fakt, że dostarczone rozwiązanie backupu musi być z nią w pełni zintegrowane a dostarczony sprzęt i oprogramowanie kompatybilne gdyż rozszerzy jednocześnie funkcjonalność obecnego środowiska IT m.in. pozwoli na migrację i podniesienie wersji obecnych systemów serwerowych, Zamawiający określa wprost nazwę oraz typ licencji, dopuszczając jednocześnie by dostarczono oprogramowanie równoważne wraz z oświadczeniem o jego pełnej kompatybilności z wymienionym w SWZ.

W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w SWZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w SWZ, w szczególności w zakresie:

* System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub wirtualizacyjnych.
* System operacyjny musi umożliwiać migrację maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
* System operacyjny musi umożliwiać downgrade do poprzedniej wersji rodziny systemów operacyjnych danego producenta.
* Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 3 lata.
* Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny.
* Licencja na system operacyjny nie może zawierać ograniczeń czasowych.
* Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i środowiskach wirtualnych serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
* Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
* System operacyjny musi posiadać graficzny interfejs użytkownika.
* System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:

a. zarządzania użytkownikami

b. zarządzania certyfikatami dla użytkowników

c. możliwości przydzielania praw ostępu do zasobów sieciowych

d. instalacji zdalnej oprogramowania z pakietów msi

e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows 10, 11

* System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
* System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
* System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
* System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
* Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
* System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra.
* System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra.
* System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
* System operacyjny musi posiadać wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
* System operacyjny musi posiadać możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
* System operacyjny musi posiadać możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
* System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
* System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6.
* System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny.
* System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.
* System operacyjny musi posiadać obsługę PowerShelI 5.1.
* System operacyjny musi posiada obsługę certyfikatów w Active Directory.

Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

Licencje nie mogą posiadać ograniczeń czasowych i muszą pochodzić z oficjalnego kanału dystrybucji. W przypadku oprogramowania Microsoft, Zamawiający oświadcza że jest uprawniony do nabycia licencji w wersjach edukacyjnych.

1. Licencje Windows Server STD 2022 EDU – 2 szt
2. Licencje Windows Server DataCenter 2022 16 core EDU – 6 szt
3. Licencje Windows Server 2022 RDS 1 User CAL – 5 szt.

***Dokument należy złożyć w formie elektronicznej opatrzony kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym***