**Załącznik Nr 5 Opis przedmiotu zamówienia / Parametry techniczne**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **System kopii bezpieczeństwa – 1 komplet : (nazwa, producent/model)……………………………………………………………..** | | | |
| ***Wymagane Parametry techniczne minimalne*** | ***Parametr Techniczny opcjonalny***  ***dodatkowo punktowany*** | ***Oferowane parametry techniczne zgodne z wymaganiami minimalnymi.***  ***Wpisać: TAK*** | **Dodatkowe punktowane parametry opcjonalne**  **Podać parametr opcjonalnie oferowany**  **(Uzupełnić w przypadku zaoferowania parametru opcjonalnego. Nie wpisanie parametru, będzie oznaczało brak jego zaoferowania)** |
| **Informacje ogólne**  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 negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny. | Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach  *(ilość punktów możliwych do uzyskania: 9)* |  |  |
| **Wymogi podstawowe**   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 fizyczny (minimum 2xCPU po 8 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 jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego. Zamawiający udostępni jedynie licencje na system operacyjny Windows Standard 2016/2019 w ilości sztuk 1 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 musi umożliwiać:    * Przełączenie manualne inicjalizowane przez administratora    * Przełączenie automatyczne w przypadku wykrycia awarii 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. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji. 9. 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 10. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów. 11. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania 12. 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 13. 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 14. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej 15. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ 16. 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 17. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP 18. Komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania 19. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN 20. 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). 21. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh 22. 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 23. 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. 24. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB. 25. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji. 26. 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. 27. 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 28. 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 29. 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. 30. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu. 31. 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 32. System musi zapewniać zintegrowane logowanie dla użytkownika końcowego poprzez tzw. social media (minimum poprzez Google) 33. 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. 34. System musi pozwalać na zarządzanie z 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. 35. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach 36. 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) 37. 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 38. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu. 39. 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 40. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO 41. System musi pozwalać na ustawianie haseł dostępu do nośników tzw.: media password 42. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:     * Fortanix Data Security Manager     * HashiCorp Vault     * IBM Security Key Lifecycle Manager (SKLM)     * Safenet     * StorMagic SvKMS     * Thales CipherTrust Manager     * VormetricAmazon Web Services (AWS) key management service     * Microsoft Azure Key Vault 43. 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 44. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:     * Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane     * Monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot     * Monitorowanie nietypowych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji     * 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 45. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email. 46. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez:     * Syslog serwer     * Splunk (dedykowany plug-in do Spluk dla analizy danych) 47. 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  1. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail 2. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV 3. 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 * Ilość nie zbackupowanych plików większa niż …% * Wielkość backupowanych danych większa niż …  1. Notyfikacje alertów muszą być wysyłane minimum poprzez mail. 2. Raport spełnienia wymogów SLA dla parametrów:    * Ilości dodatkowych kopii backupowych    * RTO    * RPO 3. System musi zapewniać funkcjonalność wznawiania zadań backupowych. 4. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych. 5. 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 6. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu 7. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków 8. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego. 9. 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. 10. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji. 11. 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 12. 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 13. 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     * Możliwość 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 14. 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 rozwiązań typu appliance 15. 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. 16. System musi realizować funkcjonalność weryfikacji wykonanych kopii. 17. 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 18. System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, Tintri, Kaminario, 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. 19. 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 20. System powinien umożliwiać (jako opcja) obsługę urządzeń składowania danych w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane 21. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows 22. System musi pozwalać na odtwarzanie tylko samych uprawnień do plików 23. System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) 24. 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. 25. 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 26. System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux 27. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix 28. System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Mandriva, Oracle Linux, Red Flag Linux, Scientific Linux, Ubuntu, Slackware 29. System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris 30. 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. 31. System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:  * Alibaba Cloud * Amazon * Citrix Xen * 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 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.   1. System musi wspierać wersje środowisk VMware 4.1, 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 poprzez integrację z vStorage API 2. 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 3. System musi wspierać środowisko Hyper-V dla:  * Microsoft Windows Server 2008 R2 SP1 * 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)  1. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych. 2. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V. 3. 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 4. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V 5. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:    * Hyper-V    * Vmware 6. Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure 7. 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. 8. 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. 9. Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów 10. Dla silników bazodanowych MS SQL, Oracle i SAP HANA musi istnieć mechanizm backupu logów tranzakcyjnych z częstotliwością co 1 minuta nawet w przypadku gdy serwer zarządzający systemem backupowym jest niedostępny 11. Konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interface 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 12. System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników 13. System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange 14. 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 15. System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL 16. Dla minimum mySQL i PostgresSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego 17. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle 18. Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio 19. Wsparcie dla backupu online dla minimum MS SQL Server 2005/2008/2008 R2/2012/2014/2016/2017/2019 na platformie Windows 20. Dedykowany agent bazodanowy dla backupu MS SQL (2017/2019) na platformie Linux: Ubuntu, SuSe, RHEL 21. Możliwość (jako opcja) archiwizacji danych z baz Oracle do plików XML 22. Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore) 23. Dedykowani agenci (jako opcja) do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk 24. 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 25. Możliwość backupu i odtwarzania (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365 z:     * SharePoint Online     * Exchange Online     * OneDrive     * Teams 26. Możliwość (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści z danych backupowanych (dokumenty i maile) z O365 27. 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. * System musi oferować możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły) * 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) * Wirtualny dysk - System musi oferować fukcjonalności jak: * możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły) * możliwość przesłania katalogów i plików ręcznie * możliwość udostępniani zawartości innym użytkowników także zewnętrznym * zarządzanie poprzez przeglądarkę i dedykowaną aplikację na urządzeniach minimum iOS i Android * 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)  1. 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. 2. 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 obsługiwać strategię wielowarstwowego aktywnego archiwum. Na przykład, umożliwiać przenoszenie zarchiwizowanych plików pomiędzy różnorodnymi urządzeniami pamięci masowej, w sposób zautomatyzowany przez politykę do wykonania krótko-, średnio- i długoterminowe okresów retencji, przy zachowaniu przejrzystego jedno- krokowego odzyskiwania dla użytkowników końcowych. * 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  1. System musi (jako opcja) umożliwiać rozbudowę o archiwizację poczty (minimum Exchange), archiwizacja poczty musi umożliwiać archiwizowanie maili z skrzynek pocztowych oraz archiwizowanie ruchu pocztowego (journaling lub SMTP journaling) 2. Oprogramowanie musi umożliwiać (jako opcja) pełnokontekstowo indeksować maile wraz z załącznikami oraz posiadać centralną konsolę do wyszukiwania danych i monitorowania zgodności z przepisami/normami bezpieczeństwa (compliance). 3. System musi umożliwiać (jako opcja) pełnokontekstowe indeksowania treści danych dla wybranych typów plików, indeksacja musi odbywać się dla danych znajdujących się już w systemie. 4. System musi umożliwiać (jako opcja) przeprowadzanie wielu wyszukiwań (eDiscovery) i zbierać wszystkie wyniki w jednej lokalizacji. 5. 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 6. Musi istnieć dedykowany agent do backupu online aplikacji MongoDB 7. 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. 8. 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 9. 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 10. 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 11. Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell 12. Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy 13. Agent do backupu systemów plikowych: Lustre, GlusterFS 14. Wsparcie (jako opcja) dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VIAO (VSphere APIs for I/O) 15. System musi zamierać 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 16. Monitorowanie i alertowanie klientów systemu którzy są trybie offline, a więc komunikacja z nimi przez system backupowy nie jest możliwa 17. Możliwość backupu (jako opcja) skrzynek pocztowych Google i dokumentów z Google Drive 18. Możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy 19. System musi posiadać integrację z ServiceNow o funkcjonalnościach:     * Dedykowany plugin do ServiceNow     * Możliwość zgłaszania zdarzeń backupowych i odtworzeniowych bezpośrednio z konsoli Service Now 20. Możliwość (jako opcja) rozbudowy środowiska o moduł VTL dla backupu danych po sieci SAN i LAN na dowolnym sprzęcie typu x86 21. Możliwość włączenia backupu pojedynczego pliku wieloma strumieniami 22. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk 23. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych 24. Dedykowane moduły do integracji z Terraform 25. Możliwość anonimizacji danych wrażliwych (data masking) minimum dla logów systemu wysyłanych np. do wsparcia 26. 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**   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:    * nielimitowana ilość bibliotek taśmowych i napędów fizycznych    * nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google) 6. W przypadku wielu lokalizacja licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami 7. Do dostarczonych licencji jest wymagane 36 miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim lub angielskim) zapewniające wsparcie techniczne w trybie 5 dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. 8. Zaoferowane licencje na system muszą zapewnić backup danych z środowiska o wielkości:    * środowisko maszyn wirtualnych (onpremis) wraz z aplikacjami i bazami:      1. ilość maszyn wirtualnych (onpremis) 60 sztuk    * środowisko serwerów fizycznych wraz z aplikacjami i bazami      1. ilość danych 11 TB |  |  |  |
| **Wymagana instalacja i konfiguracja aplikacji w środowisku Zamawiającego.**  -Instalacja oferowanego rozwiązania do tworzenia kopii zapasowych na dostarczanym serwerze bakup`u w ramach niniejszego postępowania.  -Konfiguracja oferowanego oprogramowania z zaleceniami Zamawiającego, wraz z instalacją odpowiednich agentów oprogramowania do tworzenia kopii zapasowych  -Wdrożenie/zaimplementowanie odpowiedniej polityki kopii zapasowych w oferowanym przez Wykonawcę oprogramowaniu,  -Przeprowadzenie testów przywrócenia z utworzonej przykładowej kopii zapasowej maszyny wirtualnej, którą wskaże Zamawiający  -Przekazanie dokumentacji powdrożeniowej (dotyczy oferowanego oprogramowania do tworzenia kopii zapasowych jak i pozostałych elementów oferowanych w niniejszym postępowaniu) |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Urządzenie pamięci masowej – 1 szt.: (nazwa, producent/model)……………………………………………………………..** | | | |
| ***Wymagane Parametry techniczne minimalne*** | ***Parametr Techniczny opcjonalny***  ***dodatkowo punktowany*** | ***Oferowane parametry techniczne zgodne z wymaganiami minimalnymi.***  ***Wpisać: TAK*** | **Dodatkowe punktowane parametry opcjonalne**  **Podać parametr opcjonalnie oferowany**  **(Uzupełnić w przypadku zaoferowania parametru opcjonalnego. Nie wpisanie parametru, będzie oznaczało brak jego zaoferowania)** |
| **Obudowa**  Obudowa o wysokości maksymalnie 2U dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |  |  |  |
| **Kontroler dyskowy**  Zainstalowane minimum dwa redundantne kontrolery pamięci dyskowej, pracujące w trybie symetrycznym Active-Active. Pod określeniem tryb Active-Active Symetryczny Zamawiający rozumie, że zasób pamięci dyskowej jest równolegle dostępny na co najmniej 4 portach należących do co najmniej 2 różnych kontrolerów pamięci dyskowej. Każdy z kontrolerów musi mieć możliwość prezentacji wszystkich wolumenów utworzonych w ramach całej pamięci dyskowej. |  |  |  |
| **Procesor**  Architektura przetwarzania danych w ramach procesów wewnętrznych na kontrolerach musi być realizowana za pomocą procesorów firmy Intel serii co najmniej Broadwell.  Każdy z kontrolerów musi być wyposażony w minimum jeden procesor, 6C każdy o mocy minimum 1.7 GHz |  |  |  |
|  | **Rozbudowa przestrzeni**  Dostarczone rozwiązanie musi umożliwiać podłączenie posiadanych przez zamawiającego innych macierzy dyskowych i przedstawienie ich jako kolejnych pul dyskowych, które można uwzględniać w automatycznych politykach migrowania danych.  Rozwiązanie musi umożliwiać podłączenie minimalnie do 64PB, połączenie to musi być realizowanie nie zależnie od typu infrastruktury sieciowej sieci SAN (FC lub iSCSI).  Do realizacji powyższej funkcjonalności dostarczone rozwiązanie musi wykorzystywać swoje kontrolery, niedopuszczalne jest stosowanie rozwiązań zewnętrznych, tak zwanych wirtualizatorów.  Licencja na powyższą funkcjonalność nie jest częścią bieżącego postępowania.  *(ilość punktów możliwych do uzyskania: 9) Punkt zostanie przyznany jedynie w przypadku zaoferowania wszystkich funkcjonalności* |  |  |
| **Zasilacz**  Dwa w pełni redundantne zasilane prądem 230V |  |  |  |
| **Porty sieciowe**  Każdy z dostarczanych kontrolerów pamięci dyskowej musi być wyposażony w co najmniej 2 interfejsów ISCSI SFP+ 10Gbps. |  |  |  |
| Dodatkowe półki dyskowe  Dostarczenie co najmniej jednej dodatkowej półki SAS na minimum 12 dysków 3.5 cala obsadzonej 12 dyskami HDD 14TB 7.2k obrotów Półka nie powinna przekraczać wysokości 2U i być dedykowana do zamontowania w szafie RACK 19” z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |  |  |  |
| Gwarancja  Co najmniej 3 lata od daty dostawy |  |  |  |
| Partycjonowanie | Wirtualizacja zasobów wewnętrznych musi umożliwiać utworzenie przynajmniej 2 wirtualnych macierzy dla przynajmniej 2 hostów, z możliwością delegowania przestrzeni, portu, przepustowości i spodziewanej wydajności. Parametry tych wirtualnych macierzy określamy poprzez ustalenie QOS dla danej usługi Hosta.  *(ilość punktów możliwych do uzyskania: 8)* |  |  |
| Dokumenty  Wymagane są oryginalne poświadczenia Producenta lub autoryzowanego dystrybutora producenta o oryginalnym pochodzeniu sprzętu z polskiego lub europejskiego kanału sprzedażowego. |  |  |  |
| **Parametry szczegółowe** Pełna wewnętrzna redundancja kontrolerów, portów wewnętrznych, zasilania, chłodzenia i ścieżek danych na poziomie minimum N+1.Możliwość uaktualniania oprogramowania systemowego bez przerywania działania pamięci dyskowej z utrzymaniem wszystkich funkcjonalności.Pamięć dyskowa musi być wyposażona w system zapewniający bezpieczne, bez utraty danych, automatyczne wyłączenie w przypadku całkowitego zaniku zasilania,Pamięć dyskowa musi umożliwiać wymianę kontrolerów, zasilaczy i wentylatorów w trybie Hot Swap - w trakcie pracy pamięci dyskowej.Pamięć dyskowa musi umożliwiać stosowania dysków Hot Spare i wymianę dysków w trybie Hot Swap.Pamięć dyskowa musi posiadać zainstalowaną pamięć cache o pojemności fizycznej co najmniej 128 GB. Nie dopuszcza się użycia pamięci cache zbudowanej w formie dysków SSD lub Flash itp.  1. Macierz dyskowa powinna posiadać funkcjonalność partycjonowania pamięci cache. Jeżeli funkcjonalność taka wymaga licencji to należy taką licencję dostarczyć.  W przypadku awarii zasilania niezsynchronizowane dane w pamięci cache muszą być zabezpieczone metodą trwałego zapisu do pamięci nieulotnej lub pamięć powinna być podtrzymana bateryjnie przez minimum 72h.Pamięć dyskowa musi umożliwiać instalację następujących interfejsów sieciowych:Co najmniej 16 interfejsów FC, każdy o przepustowości co najmniej 32 Gbps.Co najmniej 8 interfejsów iSCSI, każdy o przepustowości co najmniej 10Gbps.Oferowane funkcjonalności i parametry muszą być możliwe do zweryfikowania na ogólnie dostępnej stronie internetowej producenta w celu sprawdzenia, że oferowany produkt spełnia ww. wymagania.Dostarczone oprogramowanie i funkcjonalności muszą być udostępniane przez firmware bez modyfikacji przez Wykonawcę i jest to standardowe oprogramowanie producenta. Zamawiający nie dopuszcza takiej sytuacji, w której oprogramowanie pamięci dyskowej jest specjalnie przygotowane dla Zamawiającego.Pamięć dyskowa musi posiadać funkcjonalności zdalnej replikacji danych w trybie synchronicznym i asynchronicznym za pomocą sieci SAN oraz replikację typu Metro Cluster (równoległy dostęp do obu wolumenów w każdej parze replikacyjnej w trybie zapisu i odczytu). Oprogramowanie musi zapewniać funkcjonalność zawieszania replikacji i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zmiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora. Licencja na powyższą funkcjonalność nie jest częścią bieżącego postępowania.Pamięć dyskowa musi oferować wsparcie dla architektury dwuośrodkowej DR wykorzystującej do zarządzania oprogramowanie VMware SRM.Pamięć dyskowa musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point in time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Oferowane urządzenie musi obsługiwać minimum 262 000 kopii migawkowych (1024 per udział/dysk logiczny). Realizacja kopii migawkowych w trybie Copy-on-Write nie jest dopuszczona.Pamięć dyskowa musi umożliwiać migrację dysków logicznych pomiędzy grupami zabezpieczonymi różnymi typami RAID. Migracja odbywa się w trybie on-line bez przerywania pracy systemu/aplikacji korzystającej z danych migrowanego woluminu.Macierz musi umożliwiać konfigurację gwarancji wydajności typ QoS dla wybranych wolumenów logicznych w zakresie: wydajności w IOPS, wydajność w MB/s.Pamięć dyskowa musi umożliwiać wirtualizację posiadanych przez Zamawiającego zasobów dyskowych Jako wirtualizacje definiuje się zabieg techniczny polegający na udostępnieniu wirtualizowanych zasobów dyskowych klientom wirtualizatora z możliwością wykorzystania dodatkowych funkcjonalności specyficznych dla tego wirtualizatora, a nie posiadanych przez urządzenie wirtualizowane. Mechanizm wirtualizacji musi być wbudowany w oprogramowanie wewnętrzne oferowanej pamięci dyskowej i nie może być realizowany z wykorzystaniem dodatkowych zewnętrznych urządzeń i oprogramowania.Nie jest dopuszczalne rozwiązanie, w którym usługi protokołu Fibre Channel realizowane są w oparciu o emulację protokołu FC na wewnętrznym systemie plików pamięci dyskowej.Jeśli jest to konieczne, wraz z pamięcią dyskową muszą zostać dostarczone licencje na funkcję kontrolerów umożliwiającą wykorzystywanie obu kontrolerów pamięci dyskowej w taki sposób, aby oprogramowanie zainstalowane w systemie operacyjnym klienta (serwera do wirtualizacji pamięci dyskowej) automatyczne przełączało ścieżki do zasobów, np. w przypadku uszkodzenia portu karty HBA, przełącznika SAN, kontrolera pamięci dyskowej czy przewodu światłowodowego.Dostarczane oprogramowanie zarządzające pamięcią dyskową oraz licencje umożliwiają:stałe monitorowanie stanu macierzy przez jej producenta z wykorzystaniem połączenia internetowego i protokołu HTTPS.informowanie o wykorzystaniu zasobów dyskowych macierzy m.in. całkowitej pojemności przestrzeni dyskowej macierzy, wykorzystanej przestrzeni dyskowej, skonfigurowanej przestrzeni przydzielonej do serwerów i nie przydzielonej do serwerów oraz przestrzeni nie skonfigurowanej (wolnej);monitorowanie zasobów wykorzystujących funkcjonalność thin-provisioning i ostrzeganie z wyprzedzeniem o możliwości wyczerpania zasobów;monitorowanie stanu pracy par replikacyjnych, kopii migawkowych i klonów oraz funkcjonalności klastra active-active;bieżące monitorowanie wydajności macierzy mierzonej w operacjach IOPS (zapis i odczyt), strumieniu MB/s (zapis i odczyt) oraz czasów odpowiedzi RT (zapis i odczyt) m.in. dla poszczególnych wolumenów logicznych, puli dyskowych oraz portów;przygotowywanie raportów historycznych z okresu co najmniej 12 miesięcy zawierających informacje o wydajności mierzonej w IOPS i MB/s dla poszczególnych wolumenów logicznych i puli dyskowych.wykrywanie błędów i izolowanie uszkodzeń, monitorowanie w czasie rzeczywistym.zarządzanie macierzą z graficznego interfejsu użytkownika (GUI), linii komend (CLI) oraz programowego REST API.monitoring i analizę wydajności systemu pamięci masowej (również macierzy firm trzecich), przełączników SAN oraz serwerów.monitorowanie parametrów wydajnościowych w zakresie co najmniej IOPS, MB/s oraz czasów odpowiedzi RT i raportowanie przekroczenia zdefiniowanych progów.korelację zmian parametrów wydajnościowych ze zmianami konfiguracji w środowisku.generowanie alertów dla administratora przez e-mail, SNMPwykorzystanie zewnętrznych serwerów uwierzytelniania użytkowników: MS AD/LDAP |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Biblioteka taśmowa LTO – szt. 1: (nazwa, producent/model)……………………………………………………………..** | | | |
| ***Wymagane Parametry techniczne minimalne*** | ***Parametr Techniczny opcjonalny***  ***dodatkowo punktowany*** | ***Oferowane parametry techniczne zgodne z wymaganiami minimalnymi.***  ***Wpisać: TAK*** | **Dodatkowe punktowane parametry opcjonalne**  **Podać parametr opcjonalnie oferowany**  **(Uzupełnić w przypadku zaoferowania parametru opcjonalnego. Nie wpisanie parametru, będzie oznaczało brak jego zaoferowania)** |
| Wykorzystana technologia  LTO-8 Ultrium wspierające technologię partycjonowania nośników. Urządzenie musi mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO szóstej, siódmej i dziewiątej generacji |  |  |  |
| Wbudowane napędy  Dwa napędy LTO-8 wyposażone w złącze z interfejsem FC 8GB. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO z interfejsem dual SAS 6Gb oraz wspierać technologię LTFS (Linear Tape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu LTO-8 bez kompresji – minimum 300 MB/sek. Zainstalowane napędy powinny mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oraz stosować szyfrowanie danych metodą AES 256-bit |  |  |  |
| Ilość slotów i magazynki  Minimum 24 kieszenie na taśmy (urządzenie musi być dostarczone z kompletem magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot powinna odbywać się bez konieczności wysuwania całego magazynka. |  |  |  |
| Pojemność  Pojemność bez kompresji – minimum 288TB |  |  |  |
| Obudowa  Typu rack 19”. Wszystkie elementy do montażu winny być dostarczone wraz z urządzeniem, wysokość maksymalnie 2U |  |  |  |
| Zarządzanie  Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI. |  |  |  |
| Dodatkowe interfejsy  Biblioteka musi być wyposażone w interfejs sieciowy, oraz interfejs ADI | Interfejs USB  *(ilość punktów możliwych do uzyskania: 4)* |  |  |
| Obsługa urządzenia  Wymagana możliwość wymiany napędów, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napędy jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki. |  |  |  |
| Partycjonowanie  Wymagane stworzenie 2 logicznych partycji – jeżeli do tej operacji konieczna jest dodatkowa licencja, należy ją dostarczyć wraz z urządzeniem |  |  |  |
| Wyposażenie  Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli koniecznych do podłączenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabli min. 2m. Wraz z urządzeniem należy dostarczyć także zestaw nośników danych o pojemności bez kompresji minimum 12,0 TB każdy w ilości odpowiadającej ilości wszystkich dostępnych slotów na nośniki w dostarczonym urządzeniu plus 1 wraz z nośnikiem czyszczącymi, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem. Wszystkie nośniki muszą być wyposażone w naklejki z kodami kreskowymi. Instrukcja instalacji - w języku polskim lub angielskim |  |  |  |
| Gwarancja  36 miesięcy w miejscu instalacji urządzenia z czasem reakcji na zgłoszenia do 4 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia naprawy. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy wymagane do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta. Zgłaszania awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikat ISO9001 na usługi serwisowe – kontakt z serwisem w języku polskim. |  |  |  |
| Wymagana instalacja i konfiguracja urządzenia w środowisku Zamawiającego.  Montaż biblioteki w szafie RACK w pomieszczeniu udostępnionym przez Zamawiającego.  Konfiguracja biblioteki z innymi elementami infrastruktury Zamawiającego oraz dostarczanym systemem backupu |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. ***Serwer kopii bezpieczeństwa – 1 szt.* : (nazwa, producent/model)……………………………………………………………..** | | | |
| ***Wymagane Parametry techniczne minimalne*** | ***Parametr Techniczny opcjonalny***  ***dodatkowo punktowany*** | ***Oferowane parametry techniczne zgodne z wymaganiami minimalnymi.***  ***Wpisać: TAK*** | **Dodatkowe punktowane parametry opcjonalne**  **Podać parametr opcjonalnie oferowany**  **(Uzupełnić w przypadku zaoferowania parametru opcjonalnego. Nie wpisanie parametru, będzie oznaczało brak jego zaoferowania)** |
| Obudowa   * Typu RACK, wysokość nie więcej niż 2U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej; * Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; * Możliwość zainstalowania 16 dysków twardych hot plug 2,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Zainstalowane 2 szt. dysków SSD SATA 960GB Hot-Plug; * Możliwość zainstalowania wewnętrznego napędu LTO; | * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray;   *(ilość punktów możliwych do uzyskania: 3)* |  |  |
| Płyta główna   * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji procesorów 38-rdzeniowych; * Zainstalowany moduł TPM 2.0; * 7 złącz PCI Express generacji 4 w tym:   + 4 fizyczne złącza o prędkości x16;   + 3 fizyczne złącza o prędkości x8;   + Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;   + Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; * 32 gniazda pamięci RAM; * Obsługa minimum 4TB pamięci RAM DDR4; * Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna * Wsparcie dla technologii:   + Memory Scrubbing   + SDDC   + ECC   + Memory Mirroring   + ADDDC; * Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)   Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; |  |  |  |
| Procesory   * Jeden procesor 12-rdzeniowy * Taktowanie 2,1GHz * architektura x86\_64   osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 189 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/cpu2017.html> |  |  |  |
| Pamięć RAM   * 64 GB pamięci RAM * DDR4 Registered * 3200Mhz |  |  |  |
| Kontrolery LAN   * Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; * Dodatkowa karta LAN 4x 10Gbit SFP+; |  |  |  |
| Kontrolery I/O  Zainstalowane dwie karty FC 16G dwuportowe |  |  |  |
| Porty   * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 2 port USB 3.0 wewnętrzne; * 2 porty USB 3.0 dostępne z tyłu serwera; * Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; |  |  |  |
| Zasilanie, chłodzenie   * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W;   Redundantne wentylatory hotplug; |  |  |  |
| Zarządzanie  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   * Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera;   + Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP)   + Możliwość przejęcia konsoli tekstowej   + Możliwość zarządzania przez 6 administratorów jednocześnie   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)   + Obsługa serwerów proxy (autentykacja)   + Obsługa VLAN   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU)   + Wsparcie dla protokołu SSDP   + Obsługa protokołów TLS 1.2, SSL v3   + Obsługa protokołu LDAP   + Integracja z HP SIM   + Synchronizacja czasu poprzez protokół NTP   + Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); * Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. * BIOS UEFI w specyfikacji 2.7; | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii   + informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:     - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express     - procesory CPU     - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM     - wbudowany na płycie głównej nośnik pamięci M.2 SSD     - status karty zrządzającej serwera     - wentylatory     - bateria podtrzymująca ustawienia BIOS płyty główne     - zasilacze   (ilość punktów możliwych do uzyskania: 7 ) Punkt zostanie przyznany jedynie w przypadku zaoferowania wszystkich funkcjonalności |  |  |
| Wspierane OS   * Microsoft Windows Server 2022, 2019, 2016 * VMWare vSphere 6.7, 7.0 * Suse Linux Enterprise Server 15 * Red Hat Enterprise Linux 7.9, 8.3   Hyper-V Server 2016, 2019 |  |  |  |
| Gwarancja   * 36 miesięcy gwarancji producenta serwera w trybie on-site. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki. |  |  |  |
| Dokumentacja, inne   * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta; * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; * Zgodność z normami: CB, RoHS, WEEE, GS oraz CE; |  |  |  |
| System operacyjny  Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)   1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 6. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |  |  |  |
| Wymagana instalacja i konfiguracja urządzenia w środowisku Zamawiającego.  - Instalacja w szafie rack  - Konfiguracja serwera i dostarczanego systemu operacyjnego celem instalacji systemu backup`u dedykowanego do tworzenia kopii zapasowej (dostarczanego w ramach niniejszego postępowania) |  |  |  |