|  |
| --- |
| OPIS PRZEDMIOTU ZAMÓWIENIA - Zadanie nr 2   „System NAC, segmentacja sieci LAN, system kopii zapasowych” |
| 04/ZP/2022 |
| **System NAC** (Network Access Control) |

Uwagi i objaśnienia:

* Parametry określone jako „tak” są parametrami granicznymi. Udzielenie odpowiedzi „nie” lub innej nie stanowiącej jednoznacznego potwierdzenia spełniania warunku będzie skutkowało odrzuceniem oferty.
* Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu
* Zaoferowane rozwiązanie musi być uznane przez firmę analityczną Gartner Research. To znaczy musi być wymienione w bieżącym na moment składania oferty raporcie Market Guide for Network Access Control lub musi być wymienione w Gartner Peer Insights w kategorii Network Access Control, gdzie musi posiadać przynajmniej 100 opinii i status „Customer’s Choice”.
* Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.
* Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.

**PARAMETRY TECHNICZNE I EKSPLOATACYJNE**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | PARAMETR | **PARAMETR WYMAGANY** | **Parametr oferowany (podaje Wykonawca)** |
| **1.** | Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor) | TAK |  |
| **2.** | System musi odsługiwać minimum 200 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia | TAK |  |
| 3. | Praca jako maszyna wirtualna | TAK |  |
| 4. | Musi posiadać wbudowany serwer Radius | TAK |  |
| 5. | Musi posiadać wbudowany serwer TACACS+ (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie) | TAK |  |
| 6. | Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:   * Cisco Systems * Fortinet * Microsoft * Alcatel-lucent Enterprise * Aruba Networks * Huawei * Extreme Networks * PaloAlto * Netgear | TAK |  |
| 7. | System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera. | TAK |  |
| 8. | System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. | TAK |  |
| 9. | Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych. | TAK |  |
| 10. | Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych   * Microsoft Active Directory * Radius * Kerberos * LDAP * ODBC * Współpraca z serwerami tokenów | TAK |  |
| 11. | Musi obsługiwać metody profilowania (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie):   * DHCP * TCP * MAC OUI * SNMP * Cisco device sensor | TAK |  |
| 12. | Wspierać protokoły   * Radius, Radius CoA, TACACS +, web authentication, SAML v2.0 * EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS) * PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD) * TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP) * EAP-TLS * PAP, CHAP, MSCHAPv1 i v2, EAP-MD5 * NAC, Microsoft NAP * Windows machine authentication * MAC Auth * Audit (role oparte na porcie oraz skanowanie podatności) * OCSP (Online Certificate Status Protocol) * SNMP generic MIB, SNMP private MIB * CEF (Common Event Format), LEEF (Log Event Extended Format) * TLS 1.2 | TAK |  |
| 13. | Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie) | TAK |  |
| 14. | Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:   * Co najmniej ESX 4.0, ESXi 4.1 do 6.0 * Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise | TAK |  |
| 15. | Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (200). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte. | TAK |  |
| **System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności** | |  |  |
| 1. | Samodzielna rejestracja klientów gościnnych w oparciu o:   * Adres e-mail * Numer telefonu (wiadomość SMS) * Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link) | TAK |  |
| 2. | Logowanie w oparciu o portale społecznościowe | TAK |  |
| 3. | Funkcja integracji z systemami trzecimi poprzez API | TAK |  |
| 4. | Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową | TAK |  |
| 5. | Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych. | TAK |  |
| 6. | Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych. | TAK |  |
| 7. | Funkcja personalizacji strony gościnnej | TAK |  |
| 8. | Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji. | TAK |  |
| 9. | Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT | TAK |  |
| 10. | System musi wspierać obsługę następujących systemów operacyjnych   * MS Windows * Mac OS X * iOS * Android * Chromebook * Ubuntu | TAK |  |
| 11. | Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci | TAK |  |
| 12. | Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej | TAK |  |
| 13. | Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu. | TAK |  |
| 14. | Funkcja tworzenia unikalnych certyfikatów dla urządzeń. | TAK |  |
| 15. | Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń | TAK |  |
| 16. | Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID | TAK |  |
| 17. | Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji | TAK |  |
| **System kontroli końcówek klienckich musi mieć następujące funkcjonalności** | |  |  |
| 1. | System musi wspierać następujące systemy operacyjne   * Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis) * Apple Mac OS X 10.7 i nowsze * Red HAT Enterprise Linux 4 i nowsze * CentOS 4 (Community Enterprise Operating System) i nowsze * Fedora Core 5 i nowsze * SUSE linux 10.x i nowsze | TAK |  |
| 2. | Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall | TAK |  |
| 3. | Wyświetlanie informacji on-line o statusie monitorowanych końcówek | TAK |  |
| 4. | System powinien obsługiwać agenta w formie   * Stałej (Presistent Agent) * Tymczasowej (Dissolvabe Agent) * Agenta NAP | TAK |  |
| **GWARANCJA** | |  |  |
| 1. | Minimum 3 letnia gwarancja (serwis) producenta. | TAK |  |
| 2. | Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. | TAK |  |
| 3. | Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. | TAK |  |
| **SZKOLENIA** | | | |
| 1 | Przeprowadzenie instruktarzu z obsługi i konfiguracji wdrożonego oprogramowania. | TAK |  |
| **DOKUMENTACJA** | | | |
| 1 | Dostarczenie dokumentacji powdrożeniowej systemu | TAK |  |

|  |
| --- |
| Wykonanie Segmentacji i rekonfiguracji sieci LAN wraz z dostarczeniem licencjami do UTM |

Uwagi i objaśnienia:

Zamawiający posiada następujący sprzęt aktywny sieci w postaci przełączników sieciowych, rdzeniowych, przełączników dostępowych oraz klastra urządzeń bezpieczeństwa sieci klasy UTM generacji drugiej:

* przełączniki sieci LAN – Netgear gs752ts 4szt, Gs728tp 7szt, xsm7224 1 szt;
* UTM Fortigate 80F – 3 szt
* Punkty dostępowe netgear wndap 360 15szt,

**PARAMETRY TECHNICZNE I EKSPLOATACYJNE**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | PARAMETR | **PARAMETR WYMAGANY** | **Parametr oferowany (podaje Wykonawca)** |
| 1. | W ramach realizacji zamówienia usług wdrożeniowych, Wykonawca wykona plan oraz harmonogram wdrożenia obejmujący rekonfigurację posiadanej przez Zamawiającego infrastruktury teleinformatycznej a w szczególności urządzeń aktywnych sieci oraz urządzeń bezpieczeństwa sieci. W ramach usługi rekonfiguracji, Wykonawca dokona pełnej inwentaryzacji zainstalowanego sprzętu sieciowego, serwerowego oraz bezpieczeństwa sieci w sposób pozwalający na prawidłowe przygotowanie planu wdrożenia. Plan wdrożenia musi przewidywać osiągnięcie celu jakim jest poprawa bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego z wykorzystaniem posiadanego przez Zamawiającego sprzętu oraz rozwiązań oraz z wykorzystaniem najlepszych praktyk stosowanych w zakresie cyber-bezpieczeństwa. Jeśli posiadane infrastruktura będzie wymagała zastosowania dodatkowych kabli lub modułów połączeniowych to Wykonawca, musi takie elementy dostarczyć w ramach realizowanej usługi rekonfiguracji infrastruktury teleinformatycznej Zamawiającego. | TAK |  |
| 2. | Wykonawca wykona ponowną konfigurację klastra urządzenia typu firewall wraz aktualizacją oprogramowania układowego do najnowszej, stabilnej wersji oraz dostarczy licencję do trzech urządzeń UTM Fortigate 80 F na okres dwóch lat. Licencje Fortigate 80 F muszą obejmować zakres :  - aktualizacje systemu urządzenia  - kontrola aplikacji  - IPS  - Antywirus  - Botnet IP/Domain  - Mobile Malware Service  - Web Filtering  - Antispam Services | TAK |  |
| 2.1. | Wymagania konfiguracyjne obejmują:  - konfiguracje klastra UTM  - konfiguracje wszystkich interfejsów sieciowych,  - konfiguracje obiektów i grup obiektów,  - ustanowienie nowych polityk firewall i odpowiednich profili bezpieczeństwa kontrolujących i prowadzących inspekcję ruchu sieciowego dla istniejących oraz nowych usług i systemów z ekspozycją zewnętrzną oraz wewnętrzną  - translację NAT,  - identyfikację użytkowników,  - routingi,  - logowanie,  - ustawienia systemowe (m.in. dostęp administracyjny wg wymagań Zamawiającego),  - konfiguracje wymaganych routingów w/g potrzeb Zamawiającego,  - konfiguracje tuneli VPN w/g koncepcji Zamawiającego (do 20 połączeń)  - aktualizacja oprogramowania układowego wszystkich przełączników aktywnych sieci do najnowszej stabilnej wersji  - segmentacja sieci zgodnie z przyjętym przez Zamawiającego podziału na podstawie planu wdrożenia, przedstawionego przez Wykonawcę  - konfiguracja stosu logicznego dla przełączników sieciowych - rdzeniowych  - adresacja IP, podział na podsieci, utworzenie VLANów, konfiguracja routingu pomiędzy vlanami,  - rekonfiguracja systemu sieci WIFI  - integracja przełączników sieciowych oraz urządzeń sieci bezprzewodowej z urządzeniami bezpieczeństwa | TAK |  |
| 3. | Wykonawca wykona również konfiguracje polityk bezpieczeństwa, a w szczególności : | TAK |  |
| 3.1. | identyfikację użytkowników sieci i egzekwowanie zasad opartych na tożsamości w sieci szpitala, | TAK |  |
| 3.2. | konfiguracje pozostałych parametrów pracy urządzeń, nie wymienionych powyżej, a uznanych przez Zamawiającego za istotne do skonfigurowania, w terminach podanych przez Zamawiającego | TAK |  |
| 4. | Wykonawca wykona testy działania urządzeń sieciowych odbędą się zgodnie z zaakceptowanym przez Zamawiającego planem i harmonogramem wdrożenia, w tym testów:  - Poprawność działania sprzętu,  - Poprawność działania skonfigurowanych sieci LAN,  - Poprawność komunikacji pomiędzy serwerami systemu, stacji klienckich  - poprawność działania urządzeń bezpieczeństwa sieci w tym testy działania wybranych reguł i polityk bezpieczeństwa | TAK |  |
| **DOKUMENTACJA** | | | |
| 1 | Dostarczenie dokumentacji powdrożeniowej systemu | TAK |  |

|  |
| --- |
| **System kopii zapasowych** |

* Dostarczenie licencji oraz konfiguracji systemu kopii zapasowych wraz dostarczeniem urządzenia klasy NAS
* Ilość dostarczonych licencji musi zapewniać możliwość wykonania kopii:
  + 15 maszyn wirtualnych
  + 2 serwerów fizycznych
  + 5 instancji bazodanowych Oracle

**PARAMETRY TECHNICZNE I EKSPLOATACYJNE**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | PARAMETR | **PARAMETR WYMAGANY** | **Parametr oferowany (podaje Wykonawca)** |
| **1. MECHANIZMY ZABEZPIECZANIA DANYCH** | | | |
| **Ogólne** | | | |
| 1.1 | Rozwiązanie musi mieć możliwość konfigurowania liczby równoległych wątków wykonujących zadania tworzenia kopii zapasowej i odtwarzania | **TAK** |  |
| 1.2 | Rozwiązanie musi umożliwiać bezagentowe (bez konieczności instalowania agenta w zabezpieczanym systemie operacyjnym) zabezpieczenie środowisk wirtualnych, kontenerowych , aplikacji, lub instancji pamięci masowej (wolumenu lub systemu plików) | TAK |  |
| 1.3 | Mechanizm tworzenia oraz odtwarzania maszyn wirtualnych musi być spójny dla wszystkich wymienionych platform wirtualizacyjnych pod kątem konfiguracji. | TAK |  |
| 1.4 | Architektura rozwiązania powinna umożliwiać skalowanie horyzontalne (ang. scale-out) komponentów realizujących proces kopii zapasowej (ang. data-mover) | TAK |  |
| 1.5 | System powinien przechowywać wszystkie metadane kopii zapasowych w relacyjnej bazie danych | TAK |  |
| 1.6 | System powinien umożliwiać konfigurację w klastrze active-passive (komponent zarządzający rozwiązaniem) | TAK |  |
| 1.7 | System powinien umożliwiać pracę w trybie autonomicznym (bez konieczności instalowania innych systemów backupów) | TAK |  |
| 1.7 | Rozwiązanie musi umożliwić zarówno ręczne odtworzenie pojedynczej maszyny wirtualnej jak I zaplanowanie masowego odtworzenia wielu maszyn wirtualnych do wskazanego z góry środowiska (na żądanie oraz cyklicznie  z opcją nadpisania istniejących maszyn wirtualnych) | TAK |  |
| 1.8 | Rozwiązanie powinno umożliwiać automatyczne wysyłanie raportów do centralnej bazy producenta (opcjonalnie z zawartością logów) w celu usprawnienia diagnostyki i świadczenia wsparcia przez producenta | TAK |  |
| 1.9 | Vmware vSphere/ESXi |  |  |
| 1.10 | Obsługa Vmware vSphere/ESXi od wersji 6 korzystając z „VMware vSphere Storage API”. | TAK |  |
| 1.11 | Wykonywanie kopii zapasowych w oparciu o technologie NBD & HotAdd. | TAK |  |
| 1.12 | Wykonywanie przyrostowych kopii zapasowych z wykorzystaniem mechanizmu CBT. | TAK |  |
| 1.13 | Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji | TAK |  |
| 1.14 | Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej | TAK |  |
| 1.15 | Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI. | TAK |  |
| 1.16 | Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej | TAK |  |
| 1.17 | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK |  |
| 1.18 | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi. | TAK |  |
| 1.19 | Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej. | TAK |  |
| 1.20 | Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane) | TAK |  |
| 1.21 | Możliwość użycia migawek spójnych na poziomie aplikacji (ang. quiesced snapshot) przy wykonywaniu kopii zapasowej | TAK |  |
| 1.22 | Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania. | TAK |  |
| **Oracle VM** | | | |
| 1.23 | Obsługa Oracle VM od wersji 3.4 wzwyż. | TAK |  |
| 1.24 | Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji | TAK |  |
| 1.25 | Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej | TAK |  |
| 1.26 | Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI. | TAK |  |
| 1.27 | Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej | TAK |  |
| 1.28 | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK |  |
| 1.29 | Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych  w oparciu o migawki (ang. snapshot) | TAK |  |
| **AWS EC2** | | | |
| 1.30 | Wsparcie dla AWS EC2 | TAK |  |
| 1.31 | Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji | TAK |  |
| 1.32 | Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej | TAK |  |
| 1.33 | Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI. | TAK |  |
| 1.34 | Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej | TAK |  |
| 1.35 | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK |  |
| 1.36 | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi. | TAK |  |
| 1.37 | Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych  w oparciu o migawki (ang. snapshot) | TAK |  |
| 1.38 | Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej. | TAK |  |
| 1.39 | Możliwość wykonania migawki (snapshot). | TAK |  |
| 1.40 | Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania. | TAK |  |
| **Aplikacje** | | | |
| 1.41 | Rozwiązanie musi umożliwiać wykonanie kopii zapasowej przy użyciu natywnych poleceń zabezpieczanej aplikacji (wykonujących np. spójną kopię zapasową bazy danych) na zdalnych maszynach oraz poprzez opracowane dedykowane skrypty administracyjne bez konieczności wykonania obrazu całej maszyny wirtualnej lub instancji pamięci masowej (wolumenu lub systemu plików) | TAK |  |
| 1.42 | Rozwiązanie musi umożliwiać zdefiniowanie w jaki sposób kopia zapasowa będzie wykonana (jakie polecenie, jakie parametry, gdzie znajdują się pliki do zabezpieczenia) a następnie umożliwiać wielokrotne przypisanie takiej konfiguracji do wielu instancji aplikacji z różnymi wartościami parametrów, tak aby nie było konieczności wielokrotnego podawania argumentów polecenia dla każdej z aplikacji z osobna | TAK |  |
| 1.43 | Rozwiązanie musi umożliwiać wykonywanie skryptów i poleceń zarówno poprzez SSH (zdalnie) jak i z maszyny na której jest zainstalowane rozwiązanie producenta (tak, żeby nie było konieczności uruchamiania usług zdalnych takich jak SSH w celu wykonania kopii zapasowej) | TAK |  |
| 1.44 | Rozwiązanie powinno umożliwiać wkopiowanie danych backupu do innego systemu z użyciem SSH – np. transfer danych kopii zapasowej z aplikacji produkcyjnej na środowisko aplikacji testowej | TAK |  |
| **File System** | | | |
| 1.45 | Możliwość wykonywania kopii zapasowych filesystemu podłączonego do noda vProtect (katalogi, pliki zwykłe, dowiązania symboliczne) | TAK |  |
| 1.46 | Możliwość wykonania kopii zapasowej pełnej. | TAK |  |
| 1.47 | Możliwość wykonania kopii zapasowej przyrostowej. | TAK |  |
| 1.48 | Możliwość odtworzenia pojedynczego pliku. | TAK |  |
| 1.49 | Możliwość podłączenia zasobu po interfejsie ISCSI, jako dysk z filesystemem XFS. | TAK |  |
| 1.50 | Nutanix Files (AFS) | TAK |  |
| 1.51 | Możliwość wykonywania kopii zapasowych Nutanix Files (AFS), zasobów NFS/SMB, z wykorzystaniem funkcjonalności CFT. | TAK |  |
| 1.52 | Możliwość wykonania kopii zapasowej pełnej. | TAK |  |
| 1.53 | Możliwość wykonania kopii zapasowej przyrostowej. | TAK |  |
| 1.54 | Możliwość odtworzenia pojedynczego pliku. | TAK |  |
| 1.55 | Możliwość podłączenia zasobu po interfejsie ISCSI, jako dysk z filesystemem XFS. | TAK |  |
| **Ceph RBD** | | | |
| 1.56 | Możliwość wykonania kopii zapasowych wolumenów Ceph RBD. | TAK |  |
| 1.57 | Możliwość wykonania kopii zapasowej pełnej. | TAK |  |
| 1.58 | Możliwość wykonania kopii zapasowej przyrostowej. | TAK |  |
| 1.59 | Możliwość odtworzenia pojedynczego pliku. | TAK |  |
| 1.60 | Możliwość podłączenia zasobu po interfejsie ISCSI | TAK |  |
| 1.61 | Możliwość wykonywania cyklicznie migawek wolumenu bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane) | TAK |  |
| 1.62 | Możliwość automatycznego wykonania polecenia bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej. | TAK |  |
| 1.63 | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa wolumenów RBD (np. wolumeny RBD o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK |  |
| **2. SKŁADOWANIE DANYCH KOPII ZAPASOWYCH** | | | |
| **Ogólne** | | | |
| 2.1 | Rozwiązanie musi umożliwiać wykonanie polecenia/skryptu administracyjnego przed i po dostępie do pamięci masowej – np. w celu wywołania mechanizmów replikacji danych lub wysyłania powiadomień | TAK |  |
| 2.2 | Rozwiązanie musi umożliwiać synchronizację obecności kopii zapasowej  w danej lokalizacji składowania z wewnętrzna bazą danych, np. gdyby ręcznie kopie zostały usunięte, nie powinny widnieć w interfejsie użytkownika; analogicznie gdyby ponownie były dostępne, np. po tymczasowej awarii systemu plików, powinny ponownie zostać zaznaczone jako dostępne | TAK |  |
| 2.3 | System plików | TAK |  |
| 2.4 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików | TAK |  |
| 2.5 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.6 | Rozwiązanie musi oferować deduplikację danych | TAK |  |
| 2.7 | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK |  |
| 2.8 | Rozwiązanie powinno umożliwiać wykorzystanie mechanizmu ochrony nadpisania zabezpieczonych kopii zapasowych (ang. retention lock), gdy używany jest Dell-EMC PowerProtect (DataDomain) | TAK |  |
| 2.9 | System plików (syntetyczny) | TAK |  |
| 2.10 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików | TAK |  |
| 2.11 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.12 | Rozwiązanie musi umożliwiać składować dane w postaci syntetycznej bez konieczności scalania przyrostowych kopii zapasowych w trakcie odtwarzania | TAK |  |
| 2.13 | IBM Spectrum Protect | TAK |  |
| 2.14 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie IBM Spectrum Protect od wersji 7 | TAK |  |
| 2.15 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.16 | Rozwiązanie musi oferować deduplikację danych po stronie zarówno rozwiązania jak i serwera IBM Spectrum Protect | TAK |  |
| 2.17 | Dell EMC Avamar | TAK |  |
| 2.18 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Dell EMC Avamar od wersji 7.5 | TAK |  |
| 2.19 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.20 | Integracja powinna używać narzędzi administracyjnych dostarczanych przez Dell EMC | TAK |  |
| 2.21 | Dell EMC NetWorker | TAK |  |
| 2.22 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Dell EMC NetWorker od wersji 9 | TAK |  |
| 2.23 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.24 | Integracja powinna używać narzędzi administracyjnych dostarczanych przez Dell EMC | TAK |  |
| 2.25 | Veritas NetBackup | TAK |  |
| 2.26 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Versitas NetBackup od wersji 7.6 | TAK |  |
| 2.27 | Rozwiązanie musi oferować deduplikację danych po stronie serwera Veritas NetBackup | TAK |  |
| **Amazon S3, Scality S3, IBM Cloud Object Storage, Alibaba Cloud OSS, Claudian S3** | | | |
| 2.28 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie pamięci masowej oferowanej z użyciem interfejsu obiektowego S3 | TAK |  |
| 2.29 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.30 | Rozwiązanie musi umożliwiać przenoszenie starszych kopii zapasowych  z Amazon S3 do Amazon Glacier w celu redukcji kosztów przechowywania danych | TAK |  |
| 2.31 | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK |  |
| 2.32 | Rozwiązanie musi umożliwiać wsparcie dla systemów które wspierają wersjonowanie oraz takich, które nie posiadają takiej możliwości | TAK |  |
| **Microsoft Azure Blob** | | | |
| 2.33 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w chmurze pamięci masowej Microsoft Azure Blob | TAK |  |
| 2.34 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.35 | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK |  |
| 2.36 | Google Cloud Storage | TAK |  |
| 2.37 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w chmurze pamięci masowej Google Cloud Storage | TAK |  |
| 2.38 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.39 | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK |  |
| **OpenStack Swift** | | | |
| 2.40 | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie pamięci masowej oferowanej z użyciem interfejsu obiektowego Swift  w wersji 3 | TAK |  |
| 2.41 | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK |  |
| 2.42 | Rozwiązanie musi oferować kompresję danych przed składowaniem  ich w Swift | TAK |  |
| **Biblioteki Taśmowe** | | | |
| 2.43 | Obsługa bibliotek taśmowych fc/sas , mozliwość ustawienia retencji , oraz zapisu jednoprzebiegowego – kopia wykonywana raz zapisywana najpierw na dysk I potem na taśmę (disk 2 disk 2 tape) | TAK |  |
| 2.44 | Obsługa biblioteki taśmowej Dell PowerVault TL2000 z napędem LTO4 która jest w posiadaniu zamawiającego | TAK |  |
| **3 INTERFEJS ADMINISTRACYJNY I API** | | | |
| **Ogólne** | | | |
| 3.1 | Rozwiązanie musi oferować możliwość dostęp administracyjny za pośrednictwem interfejsu web’owego (przeglądarka internetowa), tekstowego (CLI) oraz API | TAK |  |
| 3.2 | Interfejsy powinny umożliwiać administratorom logowanie z użyciem poświadczeń Active Directory lub LDAP | TAK |  |
| 3.3 | System powinien umożliwiać nadawanie uprawnień i dostępów administratorom do na podstawie definiowalnych ról (ang. RBAC) na poziomie globalnym systemu (sekcji interfejsu użytkownika) oraz do poszczególnych instancji środowisk wirtualnych, aplikacji i instancji pamięci masowych (wolumenów lub systemów plików) | TAK |  |
| **Interfejs webowy** | | | |
| 3.4 | Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona | TAK |  |
| 3.5 | Interfejs musi umożliwiać wyświetlenie statystyk prędkości wykonywania kopii (ilość danych w jednostce czasu) i czasu trwania, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona z podziałem na fazy wykonywania zadań kopii zapasowych (eksport danych ze środowiska i zapis w miejscu składowania danych) | TAK |  |
| 3.6 | Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów  ze statusem ostatnio wykonanych kopii zapasowych | TAK |  |
| 3.7 | Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów  ze statusem kopii zapasowych, które nie powiodły się w ostatnim czasie –  np. w ciągu ostatnich kilkunastu minut, niedostępności komponentu wykonującego kopie zapasowe (ang. data-mover) | TAK |  |
| 3.8 | Interfejs musi umożliwiać wyświetlenie statystyk takich jak rozmiar kopii zapasowej oraz czas potrzebny na wykonanie kopii zapasowej  lub odtworzenia w perspektywie czasu, np. w celu analizy przyrostu rozmiarów backupu lub czasu jego wykonywania | TAK |  |
| 3.9 | Interfejs powinien umożliwiać raportowanie zajętość przestrzeni dyskowej w miejscach składowania danych z podziałem na środowiska wirtualne, polityki, maszyny wirtualne, instancje pamięci masowej | TAK |  |
| 3.10 | Interfejs musi umożliwiać centralne zarządzanie konfiguracją komponentów realizujących proces kopii zapasowej (ang. data-mover), danych dostępowych i metod wykonywania kopii zapasowych wirtualizatorów oraz konfiguracji miejsc składowania danych | TAK |  |
| 3.11 | Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK |  |
| 3.12 | Interfejs musi umożliwiać wykonanie odtworzenia kopii zapasowej wskazanego środowiska lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK |  |
| 3.13 | Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi również odbywać się za pośrednictwem interfejsu web’owego | TAK |  |
| 3.14 | Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych, aplikacji, instancji pamięci masowej (systemu plików lub wolumenu), migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych | TAK |  |
| 3.15 | Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać wskazywanie: godziny rozpoczęcia, dni tygodnia oraz ich kolejne wystąpienie w miesiącu (np. drugi wtorek miesiąca), miesiące | TAK |  |
| 3.16 | Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać interwałowe wykonywania zadania - wskazywanie: godziny rozpoczęcia, i godziny zakończenia i odstępu | TAK |  |
| 3.17 | Interfejs musi umożliwiać monitorowanie na żywo postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie | TAK |  |
| 3.18 | Interfejs musi umożliwiać szybkie wyszukiwanie elementów konfiguracji, środowisk wirtualnych, aplikacji i instancji pamięci masowej (systemu plików lub wolumenu) | TAK |  |
| 3.19 | Interfejs musi udostępniać kreatora konfiguracji podstawowych elementów rozwiązania takich jak dodanie środowiska wirtualnego, rozwiązań pamięci masowych, polityk i harmonogramów | TAK |  |
| 3.20 | Interfejs powinien umożliwiać wykonanie testu połączenia ze środowiskiem zabezpieczanym oraz miejsca składowania kopii zapasowych | TAK |  |
| **Interfejs tekstowy** | | | |
| 3.21 | Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona | TAK |  |
| 3.22 | Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji, lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK |  |
| 3.23 | Interfejs musi umożliwiać wykonanie na odtworzenia kopii zapasowej wskazanego środowiska lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK |  |
| 3.24 | Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi wówczas odbywać się bezpośrednio ze wskazanej ścieżki na systemie rozwiązania | TAK |  |
| 3.25 | Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych lub aplikacji, migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych | TAK |  |
| 3.26 | Interfejs musi umożliwiać monitorowanie postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie | TAK |  |
| 3.27 | Interfejs tekstowy musi być umożliwiać wykonywanie poleceń w trybie  nie-interakcyjnym (z poziomu skryptu) | TAK |  |
| **Interfejs programistyczny (API)** | | | |
| 3.28 | Rozwiązanie musi umożliwiać pełną konfigurację, wykonywanie wszystkich operacji oraz odczyt wszystkich dostępnych statystyk z poziomu API | TAK |  |
| 3.29 | Rozwiązanie musi udostępniać wszystkie API z użyciem technologii REST  i JSON | TAK |  |
| **GWARANCJA** | | | |
| 1. | Minimum 3 letnia gwarancja (serwis) producenta. | TAK |  |
| 2. | Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego na wszystkie elementy i licencje. | TAK |  |
| 3. | Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. | TAK |  |
| **SZKOLENIA** | | | |
| 1 | Wykonawca przeprowadzi instruktarz z obsługi i konfiguracji wdrożonego oprogramowania | TAK |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **URZĄDZENIE NAS** | | | | |
| **LP** | PARAMETR | **CHARAKTERYSTYKA (wymaganie minimalne** | **PARAMETR WYMAGANY** | **Parametr oferowany** |
|  |  |  |
|  | Procesor | Procesor o takowaniu nie mniejszym niż 1,7 GHz | TAK |  |
|  | Procesor liczba rdzeni | Nie mniej niż 4 | TAK |  |
|  | Pamięć RAM | Nie mniej niż 2GB DDR4 | TAK |  |
|  | Pamieć RAM liczba slotów | Minimum 1 slot | TAK |  |
|  | Pamięć RAM - możliwość rozszerzenia | nie mniej niż do 16GB | TAK |  |
|  | Pamięć Flash | Nie mniej niż 512MB | TAK |  |
|  | Liczba zatok na dyski twarde | Minimum 4 | TAK |  |
|  | Obsługiwane dyski twarde | 3.5" SATA | TAK |  |
|  | Pojemność obsługiwanych dysków twardych | do 18TB | TAK |  |
|  | Zainstalowane dyski twarde | min. Cztery dyski twarde o pojemniści min. 4TB każdy, przeznaczone do pracy w NAS w trybie 24x7, znajdujące się na liście kompatybilności producenta urządzenia o parametrach minimalnych : RPM 7200, MTBF 2 mln h, czujniki drgań obrotowych, cache 256MB, | TAK |  |
|  | Możliwość podłączenia modułu rozszerzającego | Tak, co najmniej dwóch | TAK |  |
|  | Porty LAN 2,5 Gb/s | Minimum 2 RJ-45 | TAK |  |
|  | Porty LAN 10 Gb/s | Minimum 2 na złączu SFP+ | TAK |  |
|  | Diody LED | Minimum Status, LAN, HDD, | TAK |  |
|  | Porty USB 3.2 Gen 1 | Minimum 4 | TAK |  |
|  | Port PCiE | Tak, minimum 1 | TAK |  |
|  | Przyciski | Reset, Zasilanie | TAK |  |
|  | Typ obudowy | RACK, 1U | TAK |  |
|  | Montaż w szafie | przesuwne szyny montażowe | TAK |  |
|  | Dopuszczalna temperatura pracy | od 0 do 40˚C | TAK |  |
|  | Wilgotność względna podczas pracy | 5-95% R.H. | TAK |  |
|  | Zasilanie | Minimum dwa wewnętrzne zasilacze o mocy 250 W, 100-240 V | TAK |  |
|  | Specyfikacja oprogramowania |  | TAK |  |
|  | Agregacja łączy | Tak | TAK |  |
|  | Obsługiwane systemy plików | Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ | TAK |  |
|  | Możliwość podłączenia karty WLAN na USB | Tak | TAK |  |
|  | Szyfrowanie wolumenów | Tak, min AES 256 | TAK |  |
|  | Szyfrowanie dysków zewnętrznych | Tak | TAK |  |
|  | Zarządzanie dyskami | Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,  Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T.  Skanowanie uszkodzonych bloków (pliku)  Przywracanie macierzy RAID  Obsługa map bitowych Pula pamięci masowej  Obsługa migawek  Obsługa replikacji migawek | TAK |  |
|  | Wbudowana obsługa iSCSI | Multi-LUNs na Target Obsługa LUN Mapping oraz Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S Migawka oraz kopia zapasowa iSCSI LUN | TAK |  |
|  | Zarządzanie prawami dostępu | Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie współdzieleniem w sieci  Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL | TAK |  |
|  | Obsługa Windows AD | Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP | TAK |  |
|  | Funkcje backup | Oprogramowanie do tworzenia kopii bezpieczeństwa plików, producenta urządzenia dla systemów Windows Backup na zewnętrzne dyski twarde | TAK |  |
|  | Współpraca z zewnętrznymi dostawcami usług chmury | Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box | TAK |  |
|  | Darmowe aplikacje na urządzenia mobilne | Monitoring / Zarządzanie / Współdzielenie plików / Obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android | TAK |  |
|  | Minimum obsługiwane serwery | Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu | TAK |  |
|  | VPN | VPN client / VPN server Obsługa PPTP, OpenVPN | TAK |  |
|  | Administracja systemu | Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania Ustawienia: Back up, przywracania, resetowania systemu | TAK |  |
|  | Konteneryzacja | Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker | TAK |  |
|  | Zabezpieczenia | Filtracja IP Ochrona dostępu do sieci z automatycznym adresów IP Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Zdalna replikacja Rsync Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS(bramka zewnętrzna) | TAK |  |
|  | Możliwość instalacji dodatkowego oprogramowania | Tak, sklep z aplikacjami; możliwość instalacji aplikacji z paczek | TAK |  |
|  | Maksymalna liczba użytkowników | 4096 | TAK |  |
|  | Gwarancja na urządzenie NAS | Min. 3 lata producenta | TAK |  |
|  | Gwarancja na dyski twarde | Min. 5 lat producenta, w przypadku awarii uszkodzone dyski zostają u zamawiającego. | TAK |  |

|  |
| --- |
| **System do zarządzania uprawnieniami użytkowników oraz komputerów** |

**System zostanie zainstalowany i skonfigurowany na dostarczonym przez wykonawcę sprzęcie.**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | PARAMETR | **PARAMETR WYMAGANY** | **Parametr oferowany (podaje Wykonawca)** |
| **1.** | System usługi sieciowej identyfikujący zasoby (komputery, drukarki, użytkowników, udostępnione udziały sieciowe) w sieci i udostępniający informacje o nich użytkownikom/ System zapewniający gwarancję poprawności działania, wsparcie techniczne, rozwijanie i udoskonalanie rozwiązania przez producenta do min. 2028 roku  System musi zostać dostarczony wraz z licencją pozwalającą na pracę pod kontrolą systemu min. 150 urządzeń (komputery, drukarki) jednocześnie pracujących oraz stworzenie 300 kont użytkowników którzy będę logować się na tych komputerach | TAK |  |
| **2.** | Obsługiwane protokoły transportowe   * TCP IP * NetBEUI * IPX | TAK |  |
| 3. | Usługa:  Usługa musi zapewnić pełną zgodność informacji o nazwach, opisach, lokalizacjach, dostępie, zarządzaniu i zabezpieczeniach dotyczących zasobów.  Usługa musi oferować możliwość integrowania procesów logowania do zasobów lokalnych i sieciowych oraz aplikacji użytkowych. Oznacza to tyle iż zalogowanie się do systemu zintegrowanego systemu administrowania zasobami sieci komputerowej powoduje zalogowanie się na swoje konto do aplikacji użytkowej z określonymi prawami.  Serwer dns, dhcp | TAK |  |
| 4. | Integracja z usługą DNS - usługa musi korzystać z konwencji nazewnictwa DNS przy tworzeniu struktury hierarchicznej zapewniającej znany, uporządkowany i skalowalny widok połączeń sieciowych. | TAK |  |
| 5. | Skalowalność - usługa musi być podzielona na sekcje, dzięki czemu można przechowywać bardzo dużą liczbę obiektów. W efekcie usługę można rozbudowywać wraz ze wzrostem organizacji.  Możliwość zdefiniowania organizacji którą można rozwijać . | TAK |  |
| 6. | Centralne zarządzanie - usługa musi umożliwiać administratorom zarządzanie komputerami rozproszonymi, usługami sieciowymi oraz aplikacjami z centralnej lokalizacji, przy użyciu interfejsu do zarządzania. System musi umożliwiać również centralne sterowanie dostępem do zasobów sieciowych, dzięki czemu użytkownicy mogą uzyskać pełny dostęp do zasobów, logując się tylko jeden raz do usługi . Możliwość tworzenia procedur bezpieczeństwa takich jak wymagalność zmiany hasła min co 30 dni, złożoności i powtarzalności haseł | TAK |  |
| 7. | hierarchiczna struktura usługi musi dawać możliwość delegowania administracji nad jej określonymi segmentami. Użytkownik uwierzytelniony przez wyższy podmiot administracyjny może wykonywać zadania administracyjne w określonej części struktury. Na przykład użytkownicy mogą mieć ograniczone uprawnienia administracyjne do ustawień stacji roboczej, a kierownik wydziału może mieć prawa administracyjne do tworzenia nowych użytkowników w jednostce organizacyjnej. | TAK |  |
| 8. | Struktura logiczna usługi musi być elastyczna i umożliwiać zaprojektowanie takiej hierarchii usługi, która będzie czytelna zarówno dla użytkowników, jak i administratorów. Struktura usługi powinna zawiera następujące składniki logiczne:   * Podstawową jednostkę struktury logicznej w usłudze która będzie kolekcja komputerów określonych przez administratora, które współużytkują tę samą bazę danych zawierającą katalogi. Będzie ona charakteryzowała się unikatową nazwą i umożliwiała dostęp do centralnych kont użytkowników i grup obsługiwanych przez administratora tej jednostki. * Jednostka organizacyjna. Jednostka organizacyjna to typ zbioru , w którym można gromadzić obiekty jednostki podstawowej. Jednostka organizacyjna może zawierać obiekty, takie jak konta użytkowników, grupy, komputery, drukarki i inne jednostki organizacyjne. * Musi umożliwiać zdefiniowania zbioru składającego się z jednej lub większej liczby podstawowych jednostek struktury o identycznej konfiguracji . * Musi posiadać definicję zbioru składającego się z podstawowych jednostek struktury logicznej w usłudze , które mają wspólny, ciągły obszar nazw DNS. | TAK |  |
| 9 | Możliwość uproszczonego zarządzania często grupowanymi zasobami. - Można delegować prawa administracyjne do poszczególnych atrybutów w pojedynczych obiektach usługi , ale w tym celu zwykle używa się jednostek organizacyjnych. Użytkownik może mieć prawa administracyjne do wszystkich jednostek organizacyjnych w jednostce podstawowej lub do jednej jednostki organizacyjnej. Korzystając z jednostek organizacyjnych, można tworzyć w jednostce podstawowej zbiory, które reprezentują hierarchiczną lub logiczną strukturę organizacji. Dzięki temu można zarządzać konfiguracją oraz używać kont i zasobów, korzystając z modelu organizacyjnego | TAK |  |
| 10. | System musi posiadać konsolę służącą do tworzenia, zapisywania i otwierania narzędzi administracyjnych, które zarządzają sprzętem, oprogramowaniem i składnikami sieciowymi systemu operacyjnego . Konsola powinna być w postaci graficznej, dając możliwość uruchamiania różnych przystawek do zarządzania wieloma usługami przy użyciu jednego interfejsu. Konsola powinna dać się dostosować do preferencji ergonomicznej pracy administratora, przez wskazywanie i wybieranie określone przystawek. | TAK |  |
| **Wykonawca w ramach realizacji zadania dostarczy urządzenie na którym zostanie zainstalowany system. Urządzenie musi spełniać poniższe wymagania:** | | | |
| **1.** | Stan: nowy | TAK |  |
| **2.** | obudowa: Rack | TAK |  |
| 3. | Procesor : dwa procesory każdy min. 10 wątkowy, min taktowanie 2,20 Ghz, pamięć Cache min. 13 MB | TAK |  |
| 4. | Pamięć Ram: 64 Gb DDR4 | TAK |  |
| 5. | Dyski : min 4 szt. po min. 2,4 TB 10K Sata | TAK |  |
| 6. | interfejsy sieciowe: 2xRj45 1gb/s, 2xSFP+ | TAK |  |
| 7. | Zdalne zarządzanie : Tak | TAK |  |
| 8. | dodatkowe elementy: szyny montażowe do montażu w szafie RACK | TAK |  |
| 9. | Gwarancja 24 miesiące | TAK |  |