# System bezpieczeństwa poczty elektronicznej – 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagane parametry minimalne** | **Parametry oferowane\*** |
| **1** | **2** | **3** | **4** |
| **2** | **Wymagania ogólne** | System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Rozwiązanie musi być kompatybilne z urządzeniem UTM, które posiada Zamawiający – FortiGate-200F. |  |
| **3** | **Parametry fizyczne systemu antyspamowego** | 1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.
 |  |
| **4** | **Funkcja serwera poczty** | W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.W tym zakresie dostarczony system musi zapewniać:1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.
 |  |
| **5** | **Ogólne funkcje systemu ochrony poczty** | Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
 |  |
| **6** | **Kontrola antywirusowa i ochrona przed malware** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi w wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.
 |  |
| **7** | **Kontrola antyspamowa** | System musi zapewniać poniższe funkcje i metody filtrowania spamu:1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level).
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
 |  |
| **8** | **Ochrona przed atakami na usługę poczty** | System musi zapewniać poniższe funkcje i metody filtrowania:1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.
 |  |
| **9** | **Funkcje logowania i raportowania** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
 |  |
| **10** | **Funkcje pracy w trybie wysokiej dostępności (HA)** | System ochrony poczty musi zapewniać poniższe funkcje:1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.
 |  |
| **11** | **Aktualizacje sygnatur, dostęp do bazy spamu** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
 |  |
| **12** | **Zarządzanie** | System ochrony poczty musi zapewniać poniższe funkcje:1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
 |  |
| **22** | **Wymagane certyfikaty** | Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
 |  |
| **23** | **Wymagane licencje** | System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 60 miesięcy.  |  |
| **24** | **Gwarancja oraz wsparcie Producenta** | 1. System musi być objęty serwisem producenta przez okres min. 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
 |  |
| **25** | **Opis do wymagań ogólnych** | 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
 |  |

# Serwer pod backup 1 szt:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Spełnia TAK/NIE** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| **Procesor** | Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.4GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 229 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| **RAM** | Minimum 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| **Funkcjonalność pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling  |  |
| **Gniazda PCI** | - minimum dwa sloty PCIe x16 generacji 4  |  |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSDZainstalowane 4 dyski SSD SATA o pojemności min. 1.92TB, 2,5“ Hot-Plug.Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1.Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |  |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. |  |
| **Wbudowane porty** | 4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim. |  |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **Zasilacze** | Redundantne, Hot-Plug min. 800W każdy. |  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
 |  |
| **Diagnostyka** | Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| **System Operacyjny** | Zamawiający korzysta z rozwiązań firmy Microsoft, dlatego wymaga dostarczenia licencji MS Windows Server Standard w ilości pozwalającej na uruchomienie 2 maszyn wirtualnych z systemem Windows.  |  |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla IPv6;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
 |  |
| **Oprogramowanie do zarządzania** | * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
* integracja z Active Directory
* Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
* Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
* Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
* Szczegółowy opis wykrytych systemów oraz ich komponentów
* Możliwość eksportu raportu do CSV, HTML, XLS, PDF
* Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu.
* Grupowanie urządzeń w oparciu o kryteria użytkownika
* Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
* Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
* Szybki podgląd stanu środowiska
* Podsumowanie stanu dla każdego urządzenia
* Szczegółowy status urządzenia/elementu/komponentu
* Generowanie alertów przy zmianie stanu urządzenia.
* Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
* Integracja z service desk producenta dostarczonej platformy sprzętowej
* Możliwość przejęcia zdalnego pulpitu
* Możliwość podmontowania wirtualnego napędu
* Kreator umożliwiający dostosowanie akcji dla wybranych alertów
* Możliwość importu plików MIB
* Przesyłanie alertów „as-is” do innych konsol firm trzecich
* Możliwość definiowania ról administratorów
* Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
* Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
* Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
* Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
* Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
* Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności.
* Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu o profile
* Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
* Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
* Zdalne uruchamianie diagnostyki serwera.
* Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarzadzającym.
* Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
 |  |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019. |  |
| **Warunki gwarancji** | Minimum 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Oprogramowanie - Wirtualizator** | Zamawiający wymaga dostarczenia licencji z wykupionym wsparciem producenta na rok.1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, CoreOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
14. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
16. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
17. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
18. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
19. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
20. Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
21. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
22. Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
23. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
24. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
25. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne.
 |  |

# Deduplikator 1 szt: repozytorium backupu poczty

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany**  |
|  | Urządzenie musi być przeznaczone do de-duplikacji, dedykowane do przechowywania kopii zapasowych.  | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie będące przedmiotem zapytania musi oferować przestrzeń minimum 8TB netto (powierzchni użytkowej dedykowanej do przechowywania deduplikatów) bez uwzględniania mechanizmów protekcji, wymagane skalowanie do 172TB powierzchni netto w ramach tego samego urządzenia, rozbudowa do wymaganej pojemności powinna być możliwa poprzez dołożenie kolejnych półek z dyskami oraz odpowiednich licencji, rozbudowa nie może pociągać konieczności dołożenia dodatkowych kontrolerów, nie może być również realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń. | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi posiadać minimum: * 4 porty Ethernet 10 Gb/s RJ45 – wymagana możliwość obsługi każdym z portów protokołów CIFS, NFS, de-duplikacja na źródle;
* 4 porty Ethernet 10 Gb/s SFP+ – wymagana możliwość obsługi każdym z portów protokołów CIFS, NFS, de-duplikacja na źródle;

Oferowane urządzenie musi umożliwiać rozbudowę, o co najmniej (bez konieczności usuwania w/w portów Ethernet)* 4 porty Ethernet 25 Gb/s SFP28 – wymagana możliwość obsługi każdym z portów protokołów CIFS, NFS, de-duplikacja na źródle;
* 2 porty FC 16 Gb/s – wymagana możliwość obsługi każdym z portów protokołów VTL, de-duplikacja na źródle;
 | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami, czyli dla Ethernet:* CIFS, NFS, deduplikacja na źródle (alternatywnie OST/BOOST/CATALYST) oraz jednocześnie dla FC
* VTL, de-duplikacja na źródle (alternatywnie OST/BOOST/CATALYST) w obrębie oferowanej pojemności urządzenia.
 | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagane jest dostarczenie licencji pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, VTL w przypadku pojemności oferowanego urządzenia na poziomie 172TB netto, co oznacza, że rozbudowa urządzenia z wymaganych minimum 8TB netto do 172TB netto nie może pociągać konieczności dodania kolejnych licencji w przypadku wykorzystywania protokołów CIFS, NFS, VTL w obrębie wymaganej maksymalnej pojemności urządzenia. | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagane jest dostarczenie licencji zapewniających funkcjonalność: WORM (blokada skasowania danych) w obrębie maksymalnej wymaganej pojemności urządzenia.Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem bądź modyfikacją.Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):1. umożliwiającym zdjęcia blokady przed upływem ważności danych nieumożliwiającym zdjęcia blokady przed upływem ważności danych (compliance)
 | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia. | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymaga się aby pojedyncze urządzenie dla maksymalnej pojemności osiągało zagregowaną wydajność w przypadku protokołów CIFS, NFS na poziomie co najmniej 12TB/h (dane podawane przez producenta w ogólnie dostępnych dokumentach) oraz co najmniej 27 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta w ogólnie dostępnych dokumentach). | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 270 strumieni w tym jednocześnie:* zapis danych minimum 270 strumieniami
* odczyt danych minimum 75 strumieniami
* replikacja minimum 50 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.

Wymienione wartości 395 jednoczesnych strumieni dla wszystkich protokołów, (czyli jednocześnie 270 dla zapisu, jednocześnie 75 strumieni dla odczytu oraz jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.Wszystkie zapisywane strumienie muszą podlegać globalnej de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO1, LTO2, LTO3, LTO4, LTO-5, LTO-6 | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi umożliwiać eksport oraz import definicji bibliotek taśmowych.  | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. | /Wpisać: spełnia lub nie spełnia/ |
|  | Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości.  | /Wpisać: spełnia lub nie spełnia/ |
|  | De-duplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jakie są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia w celu maksymalnego zwiększenia efektywności deduplikacji. | /Wpisać: spełnia lub nie spełnia/ |
|  | Niedopuszczalna jest de-duplikacja stałym blokiem o ustalonej tej samej długości, możliwość manulanej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku, na jaki dzielony jest każdy strumień danych. | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia. | /Wpisać: spełnia lub nie spełnia/ |
|  | Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy dowolnymi dwoma wirtualnymi bibliotekami. Blok danych otrzymany i zapisany w wirtualnej bibliotece A, nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki (wirtualnej biblioteki B) w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS) | /Wpisać: spełnia lub nie spełnia/ |
|  | Proces de-duplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. | /Wpisać: spełnia lub nie spełnia/ |
|  | Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). | /Wpisać: spełnia lub nie spełnia/ |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane jedną z metod do wyboru przez klienta: gz, lz. | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: HP Data Protector, IBM TSM, VERITAS NetBackup, DELL EMC Networker, DELL EMC Avamar, Oracle RMAN, IBM BRMS, IBM Data Studio, VMware VDP, SAP BR\*Tools, SAP HANA Studio, Microsoft SQL Server Management Studio, Veeam. | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesyłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. | /Wpisać: spełnia lub nie spełnia/ |
|  | W przypadku przyjmowania backupów z innych systemów backupu np.: VERITAS NetBackup, DELL EMC NetWorker, Oracle RMAN, Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), IBM DB2 (przy wykorzystaniu IBM Data Studio), SAP/Oracle (przy wykorzystaniu SAP BR\*Tools), SAP HANA (przy wykorzystaniu SAP HANA STUDIO), Veeam urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC (po rozbudowie o porty FC). De-duplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nieznajdujące się dotychczas na urządzeniu. | /Wpisać: spełnia lub nie spełnia/ |
|  | Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i inkrementalnych musi być wykonywane z poziomu aplikacji VERITAS NetBackup, EMC NetWorker | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia ze swojej rodziny produktowej. Wymagane są następujące tryby pracy replikacji:* jeden do jednego
* wiele do jednego
* jeden do wielu
* kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).

Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu, rozwiązanie replikacyjne nie powinno wymagać, aby obszar, na który dane są replikowane był większy od obszaru źródłowego (replikowanego) w przypadku schematu „jeden do jednego” – weryfikacja na podstawie ogólnie dostępnej dokumentacji producenta oraz zaleceń. Ewentualna licencja na replikację musi być dostarczona w ramach niniejszego postępowania. | /Wpisać: spełnia lub nie spełnia/ |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. | /Wpisać: spełnia lub nie spełnia/ |
|  | Każda grupa RAID (wymagana RAID 6) musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych półkach, w przypadku wyczerpania w nich dysków hot-spare. | /Wpisać: spełnia lub nie spełnia/ |
|  | Łącznie oferowane urządzenie musi posiadać zapasowe dyski typu hot-spare. | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania). | /Wpisać: spełnia lub nie spełnia/ |
|  | Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego poprzez:* CIFS
* NFS
* VTL

wymagany protokół umożliwiający deduplikację na źródle | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi umożliwiać przechowywanie danych niezmienialnych:* Video
* Grafika
* Nagrania dźwiękowe
* Pliki pdf

na udziałach CIFS/NFS.Wymagane jest formalne wsparcie producenta dla przechowywania powyższych danych na urządzeniu, dodatkowo wymagane jest formalne wsparcie producenta dla:* przechowywania na urządzeniu minimum 500 milionów plików dziennego zasilenia urządzenia na poziomie minimum 500 tysięcy plików
 | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagana gotowość do pracy urządzenia tzn.: możliwość zapisu oraz odtwarzania danych (przy założeniu równoległego wykorzystania wszystkich wymaganych interfejsów) po niespodziewanym wyłączeniu prądu i ponownym uruchomieniu, w czasie nie dłuższym niż 60 minut od włączenia. | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi weryfikować wszystkie zabezpieczane dane podczas procesu zapisu (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie, opisana funkcjonalność powinna być częścią procesu zapisywania danych co oznacza, że weryfikacja realizowana podczas produkcyjnego dostępu do danych (w trakcie procesu RESTORE) a nie podczas procesu zapisu danych na urządzeniu - nie spełnia niniejszych wymagań. Powyższa weryfikacja musi odbywać się w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.  | /Wpisać: spełnia lub nie spełnia/ |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu), nie może wymagać (zgodnie z oficjalnymi zaleceniami producenta) definiowania BLACKOUT WINDOW, czyli okna czasowego dedykowanego dla procesu czyszczenia, podczas którego nie są realizowane procesy backupu / odtwarzania danych czy replikacji. | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi mieć możliwość zarządzania poprzez* interfejs graficzny dostępny z przeglądarki internetowej poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
 | /Wpisać: spełnia lub nie spełnia/ |
|  | Oprogramowanie do zarządzania musi rezydować oferowanym na urządzeniu de-duplikacyjnym.  | /Wpisać: spełnia lub nie spełnia/ |
|  | Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. | /Wpisać: spełnia lub nie spełnia/ |
|  | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Urządzenie musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postepowania. | /Wpisać: spełnia lub nie spełnia/ |
|  | Wymagane wsparcie realizowane przez producenta na okres min. 5 lat w trybie 7x24 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania sprzętowego.  | /Wpisać: spełnia lub nie spełnia/ |

# System Backupu poczty:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagane parametry minimalne** | **Spełnia TAK/NIE** |
|  | **Licencjonowanie** | 1. Oprogramowanie musi zapewnić wykonywanie kopii zapasowych dla minimum 5 maszyn wirtualnych.
2. Oprogramowanie musi być objęte tzw. licencją wieczystą – jej zakup musi umożliwić korzystanie Zamawiającemu z systemu wykonywania kopii zapasowych bez ograniczeń czasowych.
3. Oprogramowanie musi zapewnić możliwość współpracy z biblioteką taśmową podłączoną bezpośrednio do serwera kopii zapasowych.
4. Oprogramowanie musi zapewnić możliwość wykonywania kopii zapasowych online dla systemu baz danych Oracle, który posiada obecnie Zamawiający.
 |  |
|  | **Wymagania ogólne** | 1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
2. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
3. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
 |  |
|  | **Całkowite koszty posiadania** | 1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. *reverse-incremental*)
4. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
5. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
6. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
7. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy aktualizacji wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania kopii migawkowych.
10. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
11. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
12. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
13. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
14. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
15. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
16. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
 |  |
|  | **Wymagania RPO (Recovery Point Objective)** | 1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
4. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastore.
5. Oprogramowanie musi automatycznie wykrywać i usuwać kopie migawkowe tzw.-sieroty (*orphaned snapshots*), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
6. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem kopii migawkowych macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich kopii migawkowych. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
7. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
8. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
9. Oprogramowanie musi posiadać wsparcie dla NDMP
10. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
11. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
12. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
13. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuksowy system plików XFS.
14. Repozytoria oparte o XFS muszą pozwalać na niezmienność danych przez określoną ilość czasu (tzw. *Immutability*)
15. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
16. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
17. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
18. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
19. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
20. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
 |  |
|  | **Wymagania RTO (Recovery Time Objective)** | 1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
2. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
5. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
7. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
8. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
9. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
* Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
* BSD: UFS, UFS2
* Solaris: ZFS, UFS
* Mac: HFS, HFS+
* Windows: NTFS, FAT, FAT32, ReFS
* Novell OES: NSS
1. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
2. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
3. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
4. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
5. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
6. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska.
7. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych.
8. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska.
9. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych.
10. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
11. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
12. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
13. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
14. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA.
15. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
 |  |
|  | **Ograniczenie ryzyka** | 1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
2. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio z kopii migawkowych macierzowych stworzonych na wspieranych urządzeniach.
3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
4. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.
5. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
6. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
 |  |
|  | **Wsparcie/subskrypcja** | 1. Oprogramowanie musi posiadać telefoniczne wsparcie techniczne i mailowe producenta ze wsparciem minimum na 1 rok w trybie 12 godzin dziennie, od poniedziałku do piątku.
2. Oprogramowanie musi posiadać możliwość subskrypcji nowych wersji na minimum 3 lata.
 |  |

# Usługi wdrożeniowe

W ramach wykonania zadania w przedmiotowym postępowaniu, Zamawiający wymaga wykonania następujących usług związanych z dostarczanymi rozwiązaniami:

## System Bezpieczeństwa Poczty Elektronicznej

Oprócz platformy dostawca zobowiązany jest do przeprowadzenia implementacji dostarczonego rozwiązania w środowisku zamawiającego gdzie zakres obejmuje poniższe elementy:

* Uruchomienie systemu na wskazanej przez zamawiającego maszynie wirtualnej (Vmware ver.)
* Instalacja licencji
* Konfiguracja interfejsów sieciowych oraz routingu
* Rekonfiguracja wpisów DNS
* Określenie chronionej domeny
* Synchronizacja systemu z posiadanym przez zamawiającego serwerem LDAP
* Rekonfiguracja oraz przeniesienie skrzynek pocztowych z posiadanego przez zamawiającego serwera pocztowego w celu zapewnienia najwyższych standardów bezpieczeństwa i kontroli poczty elektronicznej oraz ruchu SMTP. Dostęp do nowej poczty będzie odbywał się poprzez przeglądarkę www oraz dedykowanego klienta.
* Konfiguracja reguł antyspamowych
* Konfiguracja mechanizmów antyspamowych
* Konfiguracja niezbędnych polityk do poprawnej obsługi ruchu SMTP
* Implementacja mechanizmów zapewniających bezpieczeństwo ruchu SMTP:
* Profile sesji
* Profile antywirusowe
* Kontrola treści
* Konfiguracja mechanizmów archiwizacji poczty elektronicznej
* Implementacja systemu pocztowego z centralnym system korelacji logów ze zdarzeń z systemów realizujących funkcje bezpieczeństwa krytycznej infrastruktury szpitala
* Integracja z system centralnego weryfikowania plików i ich analizy w oparciu o zastosowanie najlepszych praktyk bezpieczeństwa
* Konfiguracja centralnego punktu magazynowania widomości pocztowych w którym administrator będzie mógł samodzielnie określić, czy wiadomość narusza zaimplementowane polityki bezpieczeństwa, a jeżeli nie, będzie posiadał możliwość zwolnienia wiadomości, która następnie dotrze do adresata.
* Implementacja mechanizmów analizowania załączników a tym samym aktywne usuwanie aktywnych treści bez wpływu na integralność jej treści tekstowej
* Konfiguracja systemu bezpieczeństwa poczty elektronicznej z centralnym system zbierania zdarzeń związanych z naruszeniem polityk bezpieczeństwa oraz monitorowania urządzeń bezpieczeństwa.
* Testy poprawności działania skonfigurowanego środowiska
* Przeprowadzenie jednorazowego szkolenia z zakresu konfiguracji i administracji dostarczonego rozwiązania dla maksymalnie dwóch osób wskazanych przez Zamawiającego w wymiarze 8 godzin.
* Wykonanie dokumentacji powykonawczej z wdrożonego systemu.

# Aktualizacja firmware/bios komponentów istniejącego serwera DELL R650xs

**Wykonawca** musi zaktualizować bios/firmware wszystkich komponentów serwera do najnowszej dostępnej (i zalecanej przez producenta) wersji.

# Instalacja i konfiguracja nowego serwera

**Wykonawca** musi zamontować, podłączyć do infrastruktury LAN oraz skonfigurować zakupiony serwer zgodnie z zaleceniami producenta, najlepszymi praktykami oraz wytycznymi **Zamawiającego**.

Instalacja obejmuje:

- „upgrade” oprogramowania BIOS/firmware komponentów serwera do najnowszej dostępnej (i zalecanej przez producenta) wersji

- konfigurację interfejsu zarządzającego (Management)

- konfigurację przestrzeni dyskowej (kontroler RAID)

- instalację i konfigurację systemu wirtualizacji

- instalację i konfigurację centralnej konsoli zarządzającej środowiskiem wirtualnym

# Instalacja i konfiguracja domeny Active Directory

W ramach tego zadania **Wykonawca**:

- zainstaluje maszyny wirtualne z systemem operacyjnym MS Windows Server (po jednej na każdy z hostów fizycznych)

- zainstaluje poprawki krytyczne (Windows Update)

- skonfiguruje ustawienia TCP/IP

- zainstaluje usługę Active Directory

- skonfiguruje rolę DNS oraz usługę synchronizacji czasu (NTP)

- zaimplementuje strukturę jednostek organizacyjnych dla obiektów typu: grupa, komputer, użytkownik, dział

- utworzy konta użytkowników na podstawie listy (plik w formacie „csv”) dostarczonej przez **Zamawiającego**

- skonfiguruje prawa dostępu do zasobów (grupy zabezpieczeń, przypisanie uprawnień)

- przygotuje procedury migracji danych na stacjach roboczych/laptopów do domeny

- sprawdzi poprawność działania replikacji bazy AD i folderu SYSVOL pomiędzy kontrolerami domeny

- skonfiguruje polityki GPO („Group Policy Objects”) obejmujące najważniejsze ustawienia komputerów i kont użytkowników domenowych (np. polityka haseł)

# Migracja danych na stacjach roboczych do Active Directory

Zakres prac w tym zadaniu obejmuje:

- migrację do nowej domeny profilów kont użytkowników na 5-ciu wskazanych przez **Zamawiającego** stacjach roboczych, w taki sposób, aby dane i ustawienia aplikacji zostały zachowane

- sprawdzenie poprawności przetwarzania uprzednio skonfigurowanych polityk grupowych (GPO)

# Instalacja i konfiguracja deduplikatora dyskowego

**Wykonawca** musi zamontować, podłączyć do infrastruktury LAN oraz skonfigurować zakupiony deduplikator dyskowy zgodnie z zaleceniami producenta, najlepszymi praktykami oraz wytycznymi **Zamawiającego**.

Instalacja ma obejmować:

- „upgrade” oprogramowania BIOS/firmware komponentów deduplikatora do najnowszej dostępnej (i zalecanej przez producenta) wersji

- konfigurację interfejsu zarządzającego (Management)

- konfigurację przestrzeni dyskowej na potrzeby repozytorium składowania danych (backup)

# Instalacja oraz konfiguracja systemu backupowego

W ramach tego zadania **Wykonawca**:

- zainstaluje system backupowy na maszynie wirtualnej

- skonfiguruje komunikację z deduplikatorem dyskowym

- skonfiguruje polityki backupu (harmonogramy, retencja) dla wybranych maszyn wirtualnych

- wykona testy odtworzenia danych z deduplikatora dyskowego