



Wybór serwera poczty **On-Premise Mail Server**

przewodnik dla Biznesu i Administracji publicznej

Spis treści

1 Wstęp

- Strukturyzowana analiza – od czego zacząć?

2 Licencja – jak zoptymalizować koszty i dopasować model do potrzeb organizacji?

- Rodzaj licencji – dopasowanie do sektora i potrzeb biznesowych
- Model licencjonowania – subskrypcja czy licencja wieczysta?
- Wybór funkcjonalności i optymalizacja kosztów
- Alternatywa Open Source – czy warto?

3 Model wsparcia technicznego – kto i jak odpowiada za pomoc?

- Wsparcie techniczne producenta i dostęp do wiedzy – kluczowe aspekty dla menadżera IT
- Dostęp do społeczności i bazy wiedzy

4 Architektura serwera pocztowego – kluczowe aspekty dla skalowalności i wydajności

- Skala obsługiwanego wolumenu kont
- Środowisko multiserver – skalowalność na pierwszym miejscu
- Elastyczność rozbudowy – czy system rośnie razem z firmą?
- Jakość dokumentacji i ergonomia panelu administratora

5 Integracje systemu pocztowego – kluczowy element elastyczności IT

- Metody integracji – moduły vs. API
- Bezpieczeństwo i łatwość zarządzania integracjami
- Integracja z MS Outlook – nie tylko synchronizacja poczty

6 Bezpieczeństwo i wydajność serwera pocztowego – kluczowe aspekty wyboru

- Procedura Disaster Recovery – jak szybko przywrócić działanie serwera pocztowego?
- Stabilność systemu operacyjnego
- Możliwość rozdziału kont użytkowników na wiele Mailboxów
- Obsługa szyfrowania i bezpieczeństwo transmisji danych
- Dostępność podwójnej autoryzacji (2FA) dla użytkowników i administratorów
- Współpraca z systemami cybersecurity i ochrona przed zagrożeniami
- Historia działań producenta systemu poczty i pracy grupowej.

1.Wstęp

Wybór serwera pocztowego on-premise – kluczowe kryteria dla menadżerów IT

Decyzja o wdrożeniu dedykowanego serwera pocztowego on-premise zależy od indywidualnych potrzeb firmy w zakresie integracji oraz preferencji dotyczących zarządzania infrastrukturą IT. Istnieje kilka rozwiązań na rynku oferujących zaawansowane funkcje pracy grupowej, takich jak Zimbra, KerioConnect, IceWarp, Axigen, czy Carbonio. Każda z tych platform ma odmienną filozofię pracy i architekturę, z wyjątkiem Carbonio, które jest forkiem Zimbry, rozwijanym przez firmę Zextras.

Porównanie różnych platform pocztowych on-premise może być wyzwaniem, ponieważ każda z nich oferuje unikalne funkcjonalności, architekturę i model zarządzania. Aby dokonać świadomego wyboru, warto podejść do analizy metodycznie. Jakie obszary powinien wziąć pod uwagę menadżer IT?



Strukturyzowana analiza – od czego zacząć?

Pierwszym krokiem w ocenie dostępnych rozwiązań jest określenie kluczowych wymagań organizacji. W tym celu pomocne może być wykorzystanie **ankiety projektowej**, która – choć pierwotnie opracowana pod kątem Zimbry – obejmuje wiele uniwersalnych zagadnień istotnych dla każdego wdrożenia. Dzięki niej uzyskasz pełniejszy obraz sytuacji oraz precyzyjnie określisz potrzeby firmy w kontekście wdrożenia nowego serwera pocztowego.

[wypełnij ankietę](#)



Z ankiety powinien wyłonić się obraz obecnej sytuacji oraz koncepcji jaką można wybrać do wdrożenia nowego serwera poczty z uwzględnieniem:

- **Liczby kont** dla organizacji;
- **Ilość zgromadzonych danych pocztowych** do migracji;
- **Preferowany model dostępu do danych** (w tym klienci web, MS Outlook);
- Oczekiwań na **integracje z innymi systemami IT** lub wykorzystanie dedykowanych modułów;
- **Cyberbezpieczeństwo** (FortiMail, Spam Titan Plus, 2FA, ProofPoint, archiwum poczty) – czyli o czym jeszcze należy pamiętać projektując środowisko poczty **on-premise**.

Sprawdź swoją
sytuację

[ankieta](#)



2. Licencja – jak zoptymalizować koszty i dopasować model do potrzeb organizacji?

Wybór modelu licencjonowania serwera pocztowego to jedna z kluczowych decyzji, która wpłynie zarówno na koszty, jak i elastyczność wdrożenia. W zależności od specyfiki organizacji warto przeanalizować kilka istotnych aspektów:



Rodzaj licencji – dopasowanie do sektora i potrzeb biznesowych

- **Komercyjna** - standardowe licencje dla firm, często dostępne w różnych wariantach funkcjonalnych.
- **GOV (rządowa)** - dedykowane dla administracji publicznej, często z preferencyjnymi warunkami.
- **EDU (edukacyjna)** - przeznaczone dla instytucji akademickich i szkół, zazwyczaj z obniżoną i bardzo atrakcyjną ceną.

Model licencjonowania – subskrypcja czy licencja wieczysta?

- **Subskrypcja** - pozwala na elastyczne skalowanie użytkowników oraz dostęp do aktualizacji i wsparcia technicznego w ramach cyklicznych opłat. W dłuższym wymiarze czasowym może stanowić jednak większy koszt niż rodzaj licencji wieczystej.
- **Licencja wieczysta** - jednorazowy koszt łatwiejszy do przepracowania w ujęciu księgowym ale wymagający pamiętania o opłacaniu suportów producenta w kolejnych latach.

Wybór funkcjonalności i optymalizacja kosztów

Zakup licencji powinien być dostosowany do rzeczywistych potrzeb użytkowników. Warto zwrócić uwagę na:



1 Pakiet funkcjonalności

Różnice pomiędzy wersjami mogą obejmować integrację z MS Outlook, zaawansowane moduły bezpieczeństwa czy mechanizmy archiwizacji.

2 Planowany okres użytkowania

Czy organizacja zamierza korzystać z systemu przez długi czas, czy też przewiduje możliwą zmianę technologii w przyszłości – jak tak to kiedy?

3 Optymalizacja ceny licencji

Warto przeanalizować dostępne pakiety i modele cenowe, aby uniknąć przepłacania za niewykorzystane funkcje lub zastosować mix licencji od strony funkcjonalnej – jednocześnie obniżając koszty nabycia.



Alternatywa Open Source – czy warto?

Jeśli priorytetem jest minimalizacja kosztów, warto rozważyć wdrożenie rozwiązania **Open Source**. W przypadku Zimbry dostępnych jest kilka opcji



Gotowa skompilowana wersja Open Source – dostępna np. na zintalio.com.

zintalio.com



Samodzielna kompilacja – z wykorzystaniem kodów udostępnianych na GitHubie producenta lub skorzystanie z gotowych

Dobór licencji powinien być przemyślanym procesem, uwzględniającym zarówno koszty, jak i elastyczność zarządzania infrastrukturą pocztową.

Warto rozważyć zarówno opcje komercyjne, jak i Open Source, szczególnie jeśli organizacja poszukuje rozwiązań o wysokiej skalowalności i minimalnych kosztach utrzymania.



3. Model wsparcia technicznego – kto i jak odpowiada za pomoc?

Wsparcie techniczne producenta i dostęp do wiedzy – kluczowe aspekty dla menadżera IT

Decyzja o wyborze serwera pocztowego powinna uwzględniać nie tylko funkcjonalność systemu, ale także dostępność wsparcia technicznego i zasobów edukacyjnych. Niezależnie od tego, czy organizacja zdecyduje się na wersję komercyjną, czy Open Source, warto przeanalizować kilka kluczowych aspektów.

W zależności od modelu licencjonowania, wsparcie techniczne może być świadczone przez producenta lub zewnętrzne firmy. Podstawowe pytania, na które warto znaleźć odpowiedź:



Kto odpowiada za wsparcie?

Czy jest to oficjalny zespół producenta, autoryzowani partnerzy czy społeczność użytkowników?

Jaki jest poziom SLA (Service Level Agreement)?

Czy gwarantuje określony czas reakcji i poziom obsługi incydentów?

Jak wygląda dostęp do bazy wiedzy i dokumentacji?

Czy informacje są łatwo dostępne, czy wymagają dodatkowej subskrypcji?



Przykłady modeli wsparcia:

Zimbra Network Edition

Wsparcie techniczne producenta dostępne tylko dla płatnej edycji, z określonymi zasadami SLA

[link do zasad SLA](#)

Serwery Open Source

Wsparcie oficjalne najczęściej nie istnieje, ale użytkownicy mogą liczyć na społeczność lub firmy oferujące komercyjne wsparcie.



Dostęp do społeczności i bazy wiedzy

1

Jak wygląda społeczność wokół danego rozwiązania?

Dobrze rozwinięta społeczność użytkowników może być kluczowa dla organizacji korzystającej z wersji Open Source. Aktywne forum, dokumentacja oraz dostępność tutoriali mogą znacząco ułatwić wdrażanie i zarządzanie serwerem pocztowym.

2

Jak szczegółowe są informacje na stronie producenta?

Niektóre firmy udostępniają publiczne repozytoria błędów, roadmapy rozwoju i listy poprawek, co pozwala administratorom IT na lepsze planowanie aktualizacji. Jest to dobra praktyka i „gra” w otwarte karty – dlatego niezwykle ważne jest sprawdzenie co i jak mówi producent rozwiązania w tym obszarze.

Sprawdź



3

Dostęp do informacji o błędach i poprawkach

- Czy system posiada publiczną listę zgłoszonych błędów i ich statusu?
- Czy producent regularnie aktualizuje poprawki bezpieczeństwa?
- Jak szybko dostarczane są aktualizacje krytycznych luk?

4

Dostępność bazy wiedzy i dokumentacji

To kluczowy czynnik przy wdrażaniu i utrzymaniu systemu – warto sprawdzić, jak szczegółowe informacje udostępnia producent przed podjęciem decyzji.

4. Architektura serwera pocztowego – kluczowe aspekty dla skalowalności i wydajności

Architektura serwera pocztowego ma bezpośredni wpływ na jego wydajność, skalowalność oraz stabilność. Przed wyborem odpowiedniego rozwiązania warto przeanalizować kilka kluczowych czynników technicznych, które wpłyną na efektywność zarządzania infrastrukturą IT.

Skala obsługiwanego wolumenu kont

Jednym z podstawowych pytań, jakie należy sobie zadać, jest: **jak duże obciążenie system musi obsłużyć?** Wybór architektury powinien zależeć od:

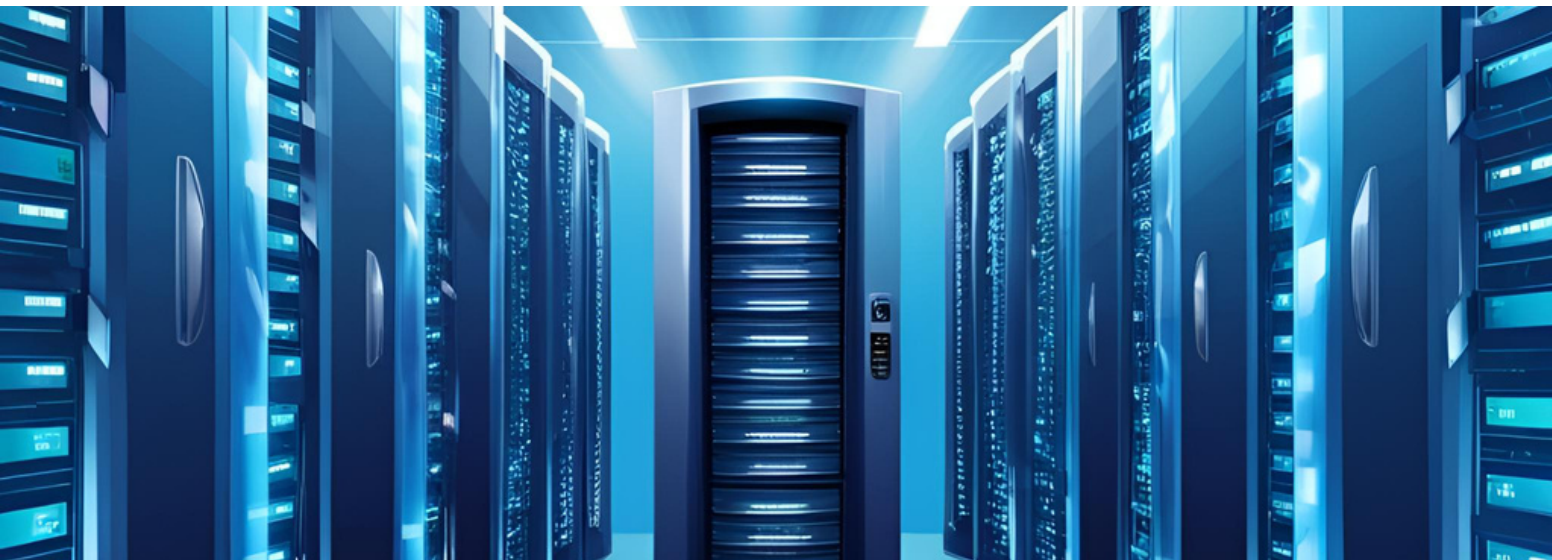


Małe i średnie firmy (do około 1500 kont) mogą funkcjonować w prostszej infrastrukturze serwera pocztowego (single server)

Duże organizacje (kilka tysięcy kont i więcej) powinny rozważyć **rozproszone środowiska wieloserwerowego (multiserver)** dla zwiększenia wydajności i niezawodności.

Środowisko multiserver – skalowalność na pierwszym miejscu

Dla większych wdrożeń warto postawić na **architekturę wieloserwerową**, która pozwala na:



Dystrybucję ruchu pomiędzy wieloma serwerami

Uniknięcie tzw. **wąskich gardeł** przy intensywnym ruchu pocztowym

Redukcję ryzyka przestojów poprzez rozdzielenie usług na dedykowane role (np. serwer pocztowy, bazodanowy, LDAP)



Przykładem może być Zimbra, która niezależnie od wersji wspiera architekturę wieloserwerową (multiserver), pozwalając na **modularne skalowanie** w zależności od potrzeb organizacji.

Elastyczność rozbudowy – czy system rośnie razem z firmą?

Organizacje rozwijające się dynamicznie powinny postawić na rozwiązania, które umożliwiają

Łatwe dodawanie nowych serwerów w ramach istniejącej infrastruktury

Obsługę środowisk chmurowych i hybrydowych i on-premise

Integrację z zewnętrznymi systemami (np. backup, archiwizacja, monitoring)

WARTO SPRAWDZIĆ

Częste aktualizacje to **większe bezpieczeństwo**, ale także **wyższe wymagania administracyjne**.
Czy producent regularnie publikuje poprawki bezpieczeństwa?

Jakość dokumentacji i ergonomia panelu administratora

Dobre rozwiązanie to takie, które można łatwo zarządzać.

- Czy producent udostępnia szczegółową dokumentację techniczną?
- Czy dostępne są przewodniki krok po kroku dla administratorów?
- Jak intuicyjny jest panel zarządzania systemem?

Dla małych i średnich firm

najlepiej sprawdzą się rozwiązania o prostej architekturze single-server z możliwością przyszłej rozbudowy

Dla dużych organizacji

kluczowe będą środowiska **multiserver**, mechanizmy **HA** oraz **wysoka skalowalność**

Regularność aktualizacji i jakość dokumentacji mogą mieć kluczowy wpływ na łatwość zarządzania i bezpieczeństwo systemu.

5. Integracje systemu pocztowego – kluczowy element elastyczności IT

Dla niektórych menadżerów IT **zdolność systemu pocztowego do integracji** jest istotnym czynnikiem wyboru, dla innych może nie mieć większego znaczenia. Jednak w dynamicznie zmieniającym się środowisku IT **elastyczność i możliwość dodawania nowych funkcjonalności** są kluczowe dla długoterminowej efektywności systemu.

Jeżeli zarządzasz infrastrukturą IT i rozumiesz wartość integracji, oznacza to, że dostrzegasz wyzwania i możliwości, jakie niesie ze sobą rozwój technologiczny. Wybór systemu pocztowego, który wspiera szeroką gamę integracji, może w przyszłości znacząco ułatwić dostosowanie środowiska do nowych potrzeb organizacji.

Metody integracji – moduły vs. API

Dedykowane moduły

gotowe rozszerzenia systemu, które można wdrożyć bez potrzeby zaawansowanej konfiguracji. Mogą one obejmować:

- ✓ Cybersecurity – filtrowanie spamu, integracja z systemami ochrony poczty (np. FortiMail, ProofPoint, SpamTitan Plus)
- ✓ Wymianę danych z innymi systemami (CRM, ERP, DMS),
- ✓ Mapowanie interfejsów użytkownika w celu uproszczenia pracy

Integracje poprzez API

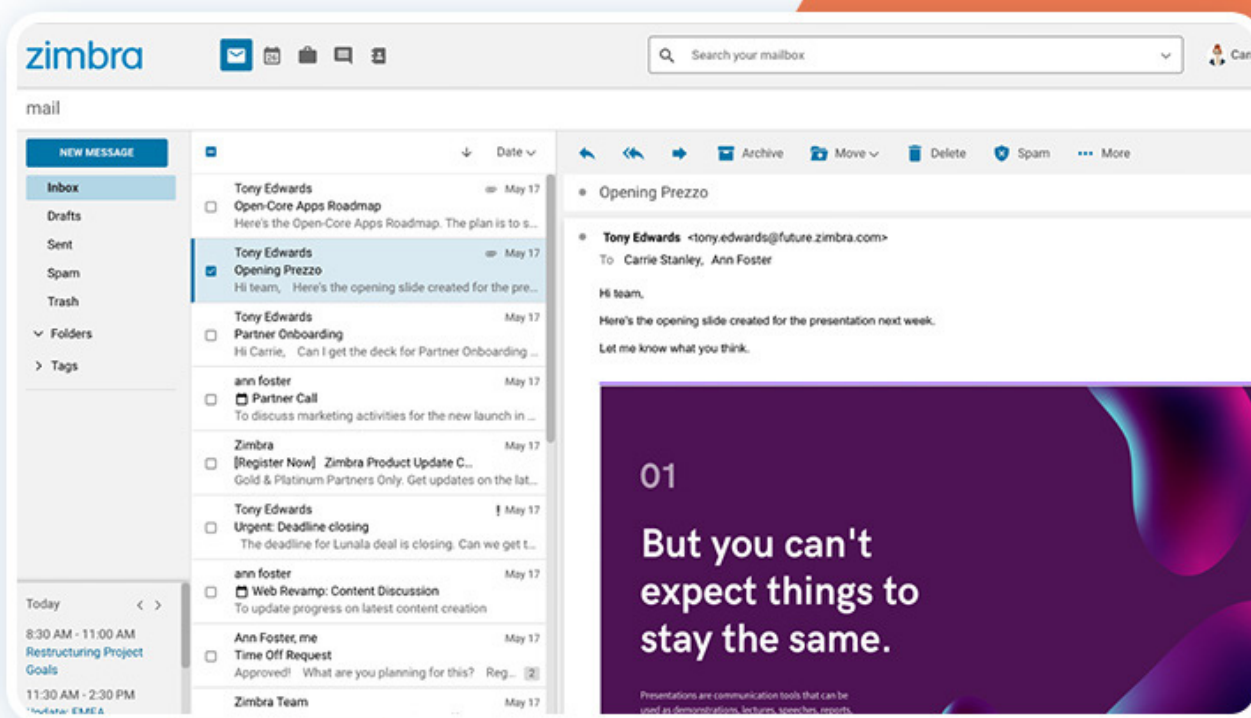
pozwalają na pełną automatyzację procesów i dostosowanie funkcjonalności systemu pocztowego do specyficznych wymagań organizacji. Dzięki API można:

- ✓ Tworzyć niestandardowe rozszerzenia, np. personalizowane powiadomienia czy synchronizację z systemami HR
- ✓ Zintegrować pocztę z wewnętrznymi aplikacjami firmy,
- ✓ Zautomatyzować procesy związane z zarządzaniem użytkownikami i skrzynkami

Bezpieczeństwo i łatwość zarządzania integracjami

Instalacja oraz zarządzanie rozszerzeniami powinny być **przejrzyste i kontrolowane**, najlepiej z poziomu **panelu administratora**, bez konieczności nadawania dodatkowych uprawnień do konsoli serwera. Takie podejście.:

- Zwiększa poziom **bezpieczeństwa**, ponieważ ogranicza dostęp do krytycznych zasobów systemu,
- Redukuje wymagania dotyczące zaawansowanej wiedzy technicznej administratorów
- Pozwala na **delegowanie zadań** w ramach zespołu IT, bez konieczności angażowania specjalistów DevOps.



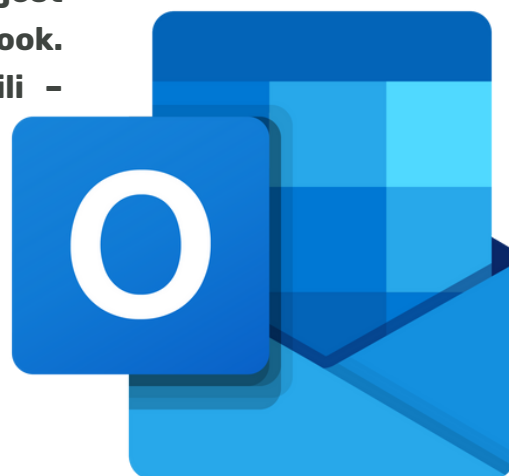
Integracja z MS Outlook – nie tylko synchronizacja poczty

Jednym z najczęstszych wymagań organizacji jest pełna współpraca systemu pocztowego z MS Outlook. Nie ogranicza się to jedynie do obsługi e-maili – równie istotne są inne funkcjonalności, takie jak:



Synchronizacja kalendarza i zadań

automatyczna wymiana informacji między serwerem pocztowym a Outlookiem



Dostęp do Globalnej Książki Adresowej
spis wszystkich użytkowników



Zarządzanie podpisami e-mail

centralne konfigurowanie stopki i jej synchronizacja z serwerem,

Monitorowanie pojemności skrzynki

informacje o wykorzystanej przestrzeni widoczne bezpośrednio w Outlooku



Automatyczne odpowiedzi (Out of Office)

synchronizacja reguł nieobecności między klientem a serwerem

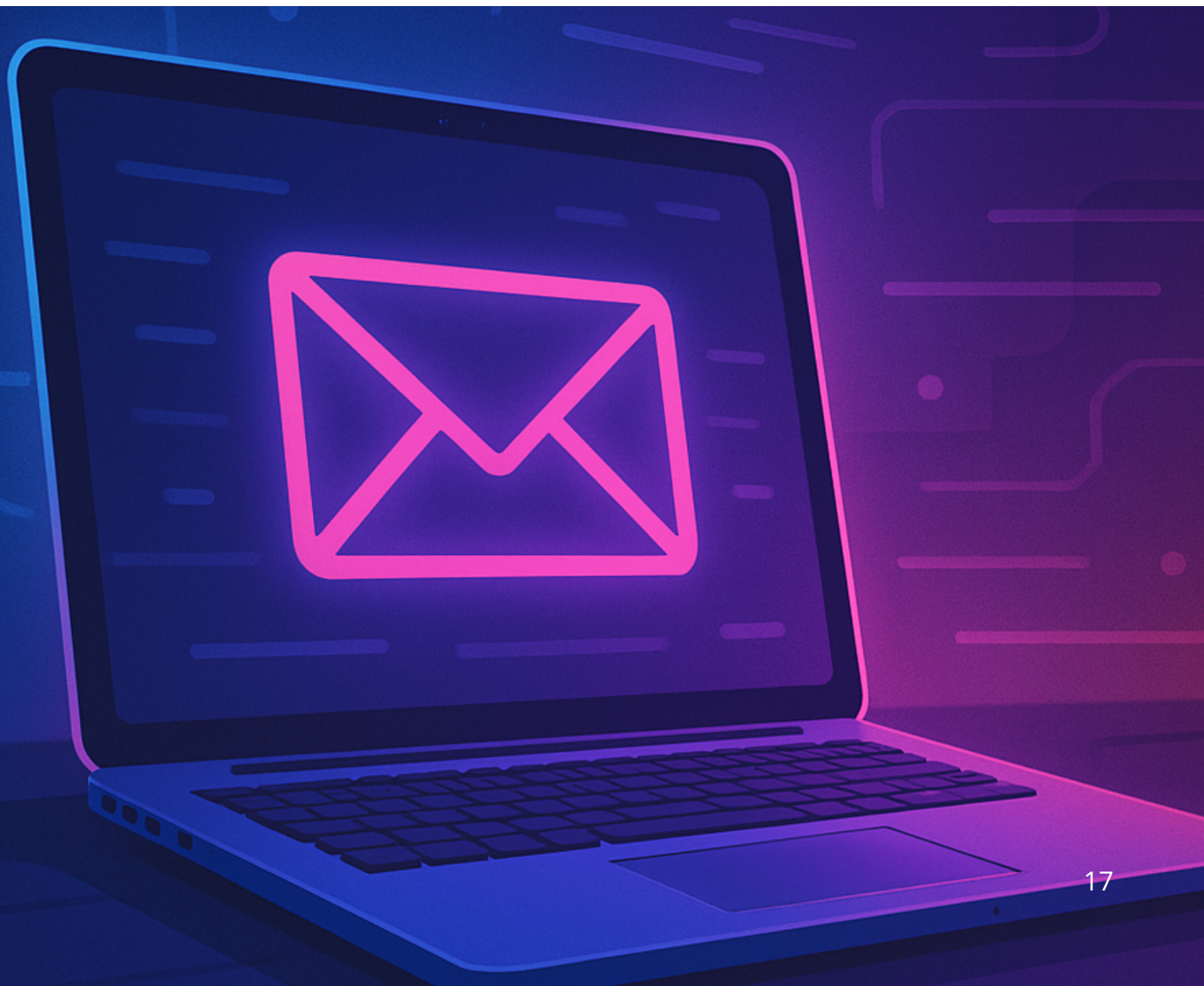
Obsługa podwójnej autentykacji (2FA)

synchronizacja reguł nieobecności między klientem a serwerem



Nie wszystkie systemy pocztowe oferują pełne wsparcie dla Outlooka – warto sprawdzić:

- Czy synchronizacja działa natywnie, czy są dedykowane przez producenta „wtyczki”?
- Jakie funkcjonalności są dostępne w integracji (tylko e-mail czy także kalendarz, kontakty i zadania)?
- Czy system obsługuje standardy **MAPI, EWS lub ActiveSync**, które są kluczowe dla efektywnej integracji z Outlookiem?



6. Bezpieczeństwo i wydajność serwera pocztowego – kluczowe aspekty wyboru

Bezpieczeństwo i niezawodność serwera pocztowego to fundament stabilnej infrastruktury IT. W dobie rosnących zagrożeń cybernetycznych oraz wymagań dotyczących ciągłości działania, wybór odpowiedniego rozwiązania powinien uwzględniać kilka kluczowych aspektów technicznych.



Procedura Disaster Recovery – jak szybko przywrócić działanie serwera pocztowego?

Awaria systemu pocztowego może sparaliżować funkcjonowanie organizacji. Dlatego niezwykle istotne jest wdrożenie skutecznych procedur **Disaster Recovery (DR)**.

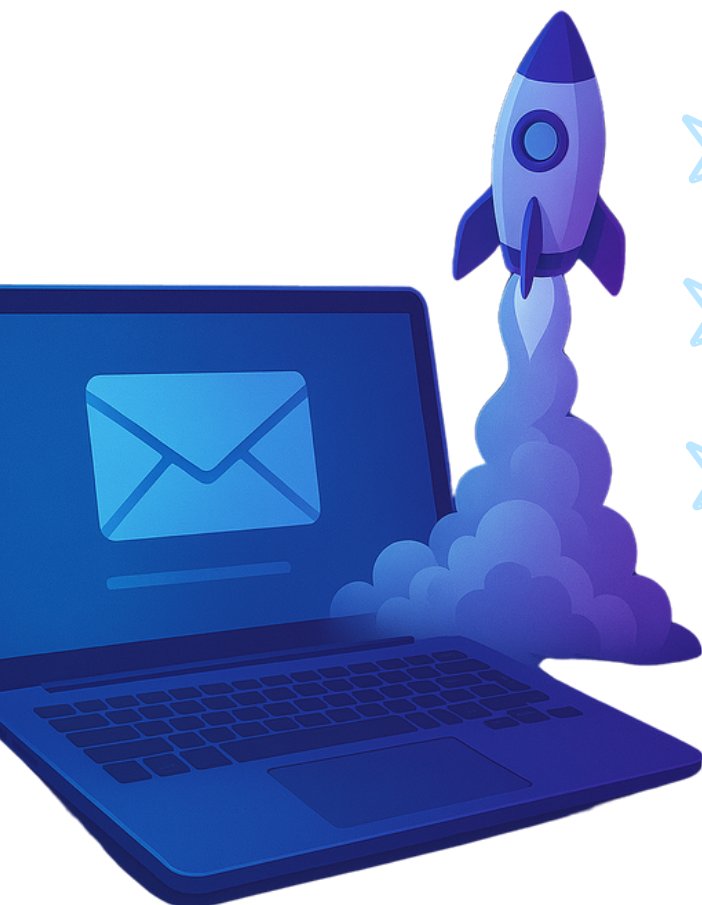
- **Czy serwer obsługuje automatyczne mechanizmy backupu?**
- **Jaka jest maksymalna akceptowalna przerwa w działaniu (RTO – Recovery Time Objective)?**
- **Jakie są mechanizmy przywracania danych (snapshoty, replikacja, backup offsite)?**

Dobre praktyki DR dla serwerów pocztowych:

- ✓ Regularne kopie zapasowe w modelu **inkrementalnym i pełnym**
- ✓ Możliwość szybkiego odtworzenia pojedynczych skrzynek lub całego środowiska
- ✓ Replikacja danych na zewnętrzne serwery (on-premise lub chmura)
- ✓ Testowanie procedur DR w celu weryfikacji ich skuteczności

Stabilność systemu operacyjnego

Niektóre systemy pocztowe działają tylko na określonych dystrybucjach Linuxa, inne oferują większą elastyczność w zakresie wyboru platformy. Warto sprawdzić:

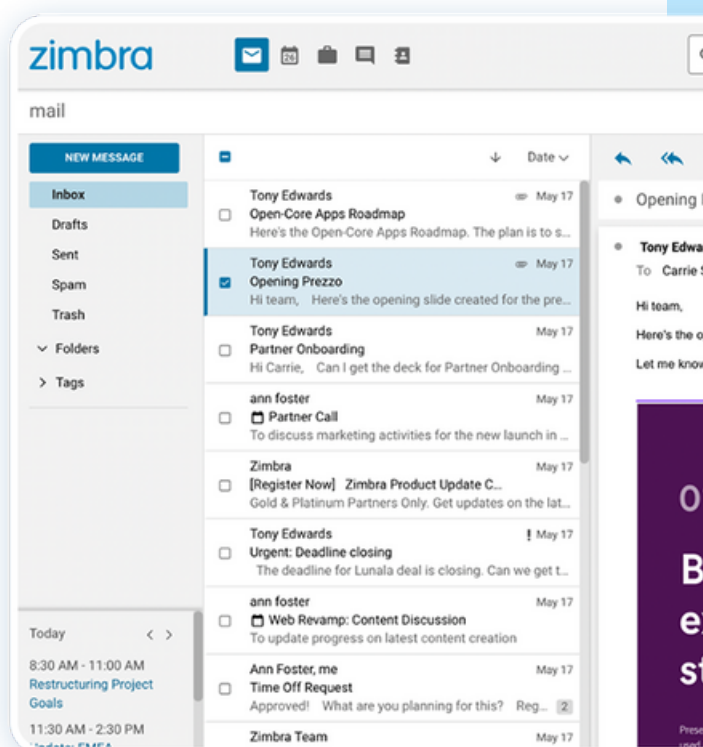


- Czy system jest wspierany na popularnych dystrybucjach (np. Ubuntu, RHEL, CentOS, Debian)?
- Jak często producent dostarcza aktualizacje i poprawki bezpieczeństwa?
- Czy wymagana wersja systemu operacyjnego nie jest przestarzała (co mogłoby stanowić zagrożenie)?

Przykłady

Zimbra obsługuje RHEL i Ubuntu (dystrybucję i pochodne), jednak nie oferuje pełnego wsparcia dla Windows Server.

Carbonio działa na wybranych wersjach Linuxa i wymaga spełnienia określonych zaleceń konfiguracyjnych.

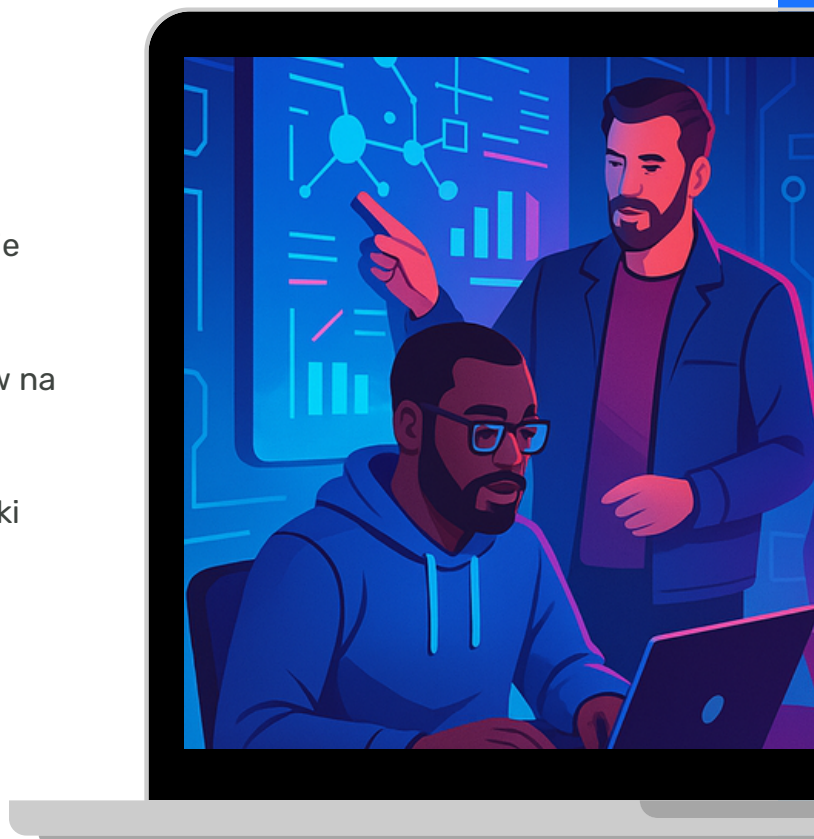


Możliwość rozdzielenia kont użytkowników na wiele Mailboxów

Dla organizacji obsługujących **dużą liczbę użytkowników (od ~1500 kont)** istotna jest możliwość podziału kont pocztowych na wiele serwerów (Mailboxów).

Zalety rozproszonej architektury Mailboxów:

- Większa skalowalność - serwer nie staje się wąskim gardłem,
- Możliwość rozdzielenia użytkowników na różne regiony/oddziały firmy,
- Wyższa odporność na awarie dzięki podziałowi obciążenia (HSM)



Obsługa szyfrowania i bezpieczeństwo transmisji danych

Szyfrowanie to podstawa bezpieczeństwa komunikacji e-mail. Każdy nowoczesny serwer pocztowy powinien obsługiwać przynajmniej jeden standard szyfrowania:

- **TLS (Transport Layer Security)**
zapewnia bezpieczne połączenie między klientem a serwerem,
- **PGP/GPG oraz S/MIME**
standardy stosowane do szyfrowania zawartości wiadomości
- **DANE (DNS-based Authentication of Named Entities)**
mechanizm zwiększający bezpieczeństwo poczty w warstwie DNS

Czy serwer wspiera szyfrowanie end-to-end (E2EE)?

Dostępność podwójnej autoryzacji (2FA) dla użytkowników i administratorów

Czy serwer obsługuje dwuskładnikowe uwierzytelnianie (2FA)?



2FA znacznie zwiększa poziom bezpieczeństwa i jest kluczowym elementem ochrony kont użytkowników.

Najczęściej stosowane metody 2FA

TOTP	YubiKey i klucze U2F	SMS / e-mail z kodem jednorazowym
(Time-based One-Time Password) aplikacje jak Google Authenticator, Microsoft Authenticator	sprzętowe tokeny do logowania	(choć mniej bezpieczne)

Współpraca z systemami cybersecurity i ochrona przed zagrożeniami

Czy serwer pocztowy można zintegrować z narzędziami zabezpieczającymi?

Serwer powinien współpracować z systemami cybersecurity, takimi jak:



Antyspam i filtrowanie treści – np. SpamTitan, FortiMail, ProofPoint lub dedykowane moduły cybersecurity

Systemy antywirusowe – automatyczne skanowanie załączników i treści wiadomości

SIEM (Security Information and Event Management) – centralna analiza logów i wykrywanie anomalii

DMARC, SPF, DKIM – zabezpieczenia przed sporingiem i phishingiem

Historia działań producenta systemu poczty i pracy grupowej

- **Czy producent posiada historię produktu?**
- Od ilu lat działa na globalnym rynku z produktem?
- Jak duże firmy korzystają na Twoim rynku z tego rozwiązania?

Podsumowanie

- ✓ **Procedury Disaster Recovery**
powinny umożliwiać szybkie przywrócenie działania systemu
- ✓ **Wybór stabilnego systemu operacyjnego**
zwiększa bezpieczeństwo i niezawodność
- ✓ **Możliwość podziału kont na wiele mailboxów**
kluczowa dla dużych organizacji
- ✓ **Szyfrowanie i 2FA**
powinny być standardem w nowoczesnych rozwiązaniach pocztowych
- ✓ **Integracja z narzędziami cybersecurity**
pozwała na skuteczną i dostosowaną w punkt ochronę przed zagrożeniami

Wybór serwera pocztowego on-premise to jak widać decyzja wymagająca analizy wielu czynników, od modelu licencjonowania po możliwości integracyjne i kwestie cyberbezpieczeństwa.

- Jeżeli chcesz dowiedzieć się więcej o najlepszych praktykach zabezpieczania serwera pocztowego lub jego skalowania?
- Potrzebujesz migrację ze starszego środowiska Zimbra?

SKONTAKTUJ SIĘ Z NAMI

Pomożemy dobrać optymalne rozwiązanie dla Twojej organizacji!