Minimalne wymagania dla instalacji onPremise/Private cloud

dla systemu Ready_™

Środowisko pracy serwera powinno zapewnić odpowiedni dla przeznaczenia systemu poziom bezpieczeństwa oraz szybkie i stabilne działanie aplikacji. W tym celu serwer, a także całe środowisko pracy, muszą spełniać odpowiednie wymagania techniczne.
Poniżej przedstawiona jest lista minimalnych wymagań, których spełnienie zapewnia uzyskanie minimalnego wymaganego standardu jakości i bezpieczeństwa.
Prosimy o zapoznanie się z wymaganiami i potwierdzenie spełnienia wszystkich minimalnych wymagań w formie załączonej checklisty. Weryfikacja nie jest konieczna w przypadku posiadania przez organizację wdrożonego systemu ISO 27001.

CHECKLISTA

Parametr	Minimalne wymaganie	x
Polityka bezpieczeństwa	W organizacji jest przyjęta i sformalizowana polityka bezpieczeństwa.	
Polityka bezpieczeństwa fizycznego	Wydzielone pomieszczenie z zabezpieczonym dostępem, wyposażone w klimatyzację.	
Polityka zarządzania kopiami	W organizacji jest przyjęta i sformalizowana polityka zarządzania kopiami bezpieczeństwa przynajmniej dla 1 serwera.	
Polityka haseł	W organizacji jest przyjęta i sformalizowana polityka haseł.	
Polityka zabezpieczenia sieci	W organizacji jest przyjęta i sformalizowana polityka zabezpieczania sieci.	
Firewall	Dostęp do sieci wewnętrznej, w której zlokalizowane są serwery chroniony jest za pomocą Firewall, dzięki czemu możliwe jest bezpieczne połączenie do zasobów integrowanych usług np. systemu ERP.	
Stały adres IP	Organizacja dysponuje dostępną pulą przynajmniej jednego wolnego stałego adresu IP.	
Możliwość konfiguracji domeny	Organizacja dysponuje dostępną domeną lub subdomeną, oraz pozwala na zdefiniowanie i wykorzystanie nazwy domenowej dla serwera.	
Certyfikaty szyfrujące	Organizacja dysponuje certyfikatami dla serwera (wydane dla domeny lub subdomeny, ewentualnie wildcard) w celu szyfrowania transmisji protokołem SSL.	
Wirtualizacja	W momencie udzielenia zamówienia dostępne jest działające środowisko wirtualizacji np. Vmware vSphere, HyperV. Nie ma przeciwskazań do instalacji systemu z przygotowanego wcześniej	

	przetestowanego, zabezpieczonego i utrzymywanego w jednej wersji obrazu systemu Debian Linux 10. W celu instalacji na innej dystrybucji wymagany jest dodatkowy przegląd i uzgodnienia w zakresie instalacji i procedur utrzymania systemu operacyjnego w długim terminie.	
Mechanizm kopii bezpieczeństwa	Kopie baz danych wykonywane są za pomocą dedykowanych narzędzi. Zalecana jest ich pełna automatyzacja lub pisemna procedura zapewniająca ich wykonywanie.	
Procedura weryfikacji	Kopie baz danych są okresowo weryfikowane pod kątem zawartości oraz prawidłowego odtworzenia w środowisku testowym.	
Storage dla kopii bezpieczeństwa	Firma dysponuje zewnętrznym zasobem przeznaczonym na wykonywanie kopii np. dysk sieciowy NAS.	
UPS	Dostępne jest zabezpieczenie serwerów przed utratą zasilania.	
Serwer na wyłączność	Na wskazanym serwerze będą zainstalowane tylko eDokumenty/Ready_™. Serwer nie będzie współdzielony z innym nieautoryzowanym oprogramowaniem.	
Procesor	Minimalnie 8 rdzeni 2.4 GHz (szczegółowe wymagania poniżej).	
Pamięć RAM	Minimalnie 16 GB (szczegółowe wymagania poniżej)	
HDD	Transfer dla bazy danych min. 500 Mbps Transfer dla plików min. 200Mbps	
RAID	Sprzętowy 5, zalecany 10	
Zasilacz	Zalecany dodatkowy zasilacz (nadmiarowy)	
Redundancja komponentów	Wymagane jest zapewnienie redundancji komponentów sprzętowych. Na wypadek awarii, każdy z komponentów powinien móc być zastąpiony w czasie nie dłuższym niż 24h. W szczególności dotyczy to dysków, zasilacza i płyty głównej.	
Postępowanie z logami	Logi serwerów są okresowo przeglądane w celu wykrycia potencjalnych problemów.	
Serwer poczty email	Serwer pocztowy obsługuje protokoły IMAP i SMTP i nie posiada ustawionych ograniczeń dotyczących liczby przyjmowanych połączeń z jednego adresu IP / dla jednego konta mailowego (wymaganie dotyczy przypadku korzystania z klienta pocztowego Ready_™)	
Zegar systemowy serwera	Zegar systemowy jest prawidłowo ustawiony (zalecane jest używanie protokołu NTP).	
Zdalny dostęp	Bezpieczny zdalny dostęp do konsoli SSH, za pomocą tunelowanego połączenia protokołu VPN, IPsec. Zalecane jest pozostawienie otwartych na świat jedynie portów usługi Apache tj. 80 (redirect na 443) i 443.	

High Availability

Konfiguracja środowiska powinna zapewnić szybkie i stabilne działanie aplikacji. Poniżej przedstawiona jest propozycja czterech konfiguracji w zależności od przewidywanej liczby użytkowników i parametrów oczekiwanej szybkości działania.
Wymagania zostały zunifikowane dla instalacji fizycznych i private cloud (VPS). Przyjęto założenie, że szczegółowe parametry procesorów oraz pamięci RAM nie odbiegają od aktualnie panujących standardów dla średniej półki cenowej sprzętu/usługi VPS.

KONFIGURACJA I

Konfiguracja zalecana dla niewielkich instalacji do 50 jednoczesnych użytkowników.

Liczba procesorów	2-4
Pamięć RAM	8-16 GB
Przestrzeń dyskowa	100-500 GB
Przestrzeń na backup	100-500 GB

KONFIGURACJA II

Konfiguracja zalecana dla instalacji około 100 jednoczesnych użytkowników i powyżej.

Liczba procesorów	4-8	Osobny serwer bazy danych	TAK
Pamięć RAM	8-24 GB		
Przestrzeń dyskowa	100GB - 1 TB		
Przestrzeń na backup	100GB - 1 TB		

KONFIGURACJA III

Konfiguracja zalecana dla instalacji znacznie przekraczających 100 jednoczesnych użytkowników, znacznie obciążonych pracą w systemie.

Liczba procesorów	4-8	Osobny serwer bazy danych	TAK
Pamięć RAM	8-24 GB	Osobny serwer OCR	TAK
Przestrzeń dyskowa	100GB - 1 TB		
Przestrzeń na backup	100GB - 1 TB		

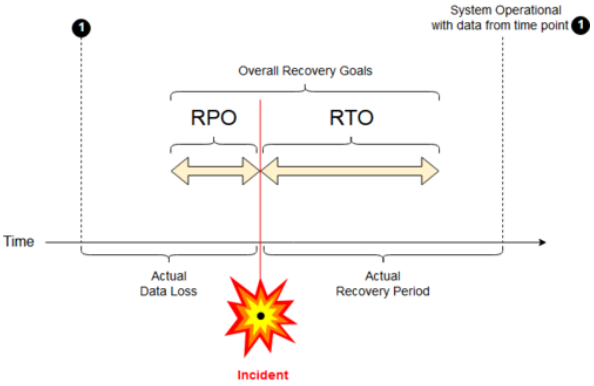
KONFIGURACJA IV

Konfiguracja zalecana dla instalacji przekraczających 500 jednoczesnych użytkowników i wysokich oczekiwań względem szybkości i wydajności przetwarzania.

Liczba procesorów	8-24	Osobny serwer bazy danych	TAK
Pamięć RAM	16-32 GB	Osobny serwer OCR	TAK
Przestrzeń dyskowa	1-2 TB	Osobny serwer kolejki i sesji	TAK
Przestrzeń na backup	1-2 TB	Load balancer i klaster	TAK

Disaster Recovery

W zależności od oczekiwanego dla zastosowania systemu maksymalnego akceptowalnego czasu potencjalnej utraty danych na skutek awarii bazy danych i konieczności jej przywrócenia z kopii zapasowej stosuje się następujące terminy:
RPO – Recovery Point Objective – Czas od wykonania ostatniej kopii do awarii
RTO – Recovery Time Objective – Czas od awarii do uruchomienia usługi po odtworzeniu



Poniżej podano kilka przykładowych oczekiwanych parametrów RPO/RTO oraz zalecanych procedur pozwalających na ich uzyskanie.

OCZEKIWANY RPO – MAX 1 DZIEŃ ROBOCZY

Czas odtworzenia RTO – 8h

Kopia zapasowa	W nocy (pełna)
Procedura odtworzenia	Odtworzenie z pełnej kopii nocnej

OCZEKIWANY RPO – MAX 15 MINUT

Czas odtworzenia RTO – 4h.

Kopia zapasowa	Tygodniowy lub nocny base backup + przyrostowa WAL
Procedura odtworzenia	Barman (do dowolnego miejsca w czasie od czasu base backup)
Dodatkowy serwer	Serwer dla kopii przyrostowych

OCZEKIWANY RPO - MAX 15 MINUT

Czas odtworzenia RTO – max 15 minut.

Kopie zapasowe	W nocy (pełna) + replikacja w czasie rzeczywistym
Procedura odtworzenia	Failover, Manualne przełączenie na slave
Replikacja	Replikacja strumieniowa (WAL) master->slave
Dodatkowy serwer	Minimum 1 dodatkowy serwer dla replik