

CHECKLISTA DIAGNOSTYCZNA

12 sygnałów, że środowisko wymaga audytu

ORACLE WEBLOGIC / IBM WEBSPHERE

Sprawdź objawy. Zbierz dowody. Ustal priorytety.

Dla administratorów, DevOps Leadów i osób odpowiedzialnych za ciągłość usług. Przy każdym sygnale znajdziesz sposób sprawdzenia oraz kryterium, kiedy nadać mu priorytet.

JAK KORZYSTAĆ

1. Oceń jedno środowisko i ostatnie 30 dni pracy.
2. Wybierz Tak, Nie lub Nie wiem przy każdym sygnale.
3. Podsumuj odpowiedzi i zapisz trzy działania na stronie 5.

Środowisko / usługa

Data przeglądu

Osoba odpowiedzialna

Zakres: WebLogic Server i WebSphere Application Server traditional. Uwzględnij też ostatnie wdrożenie i test odtworzenia. Narzędzia dobieraj do wersji serwera i JVM; Liberty wymaga odrębnego dopasowania.

01-04 / WYDAJNOŚĆ I KONFIGURACJA

Czy usługa działa przewidywalnie?

Tak = sygnał występuje. Nie wiem = wymaga sprawdzenia.

01

WĄTKI

Stuck / hung threads powracają

Regularnie pojawiają się ostrzeżenia o długim wykonaniu wątków i towarzyszą im opóźnienia lub błędy usługi.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

WLS: wyszukaj BEA-000337; WAS: WSVR0605W.
Porównaj serię zrzutów wątków z czasem odpowiedzi bazy i integracji.

KIEDY REAGOWAĆ

Ostrzeżenia powracają wraz z degradacją usługi lub blokadą pracy. Sam wpis nie dowodzi zakleszczenia.

02

JVM / GC

Pauzy GC pogarszają czas odpowiedzi

Pauzy lub udział czasu GC rosną względem normalnej pracy i naruszają oczekiwany czas odpowiedzi usługi.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Zestaw logi GC, stertę po GC, obciążenie i p95/p99.
Porównaj z okresem poprawnej pracy tej samej JVM.

KIEDY REAGOWAĆ

GC narusza wymagany czas odpowiedzi lub wyraźnie pogarsza się względem normy. Nie ma uniwersalnego progu 1 s.

03

STABILNOŚĆ

Restart zastępuje diagnozę

Usługa wraca po restarcie, lecz ten sam problem pojawia się ponownie bez potwierdzonej przyczyny.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Zachowaj logi i metryki sprzed restartu. Heap dump dobieraj do JVM (HotSpot / OpenJ9) i oceń wpływ na usługę przed wykonaniem.

KIEDY REAGOWAĆ

Problem wraca, a restart jest stałym obejściem bez diagnozy. Heap dump może zatrzymać lub obciążyć JVM.

04

DOKUMENTACJA

Konfiguracji nie da się odtworzyć

Brakuje aktualnej topologii, wykazu zasobów lub historii zmian; dokumentacja nie odpowiada produkcji.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Porównaj dokumentację z konfiguracją: topologia, JDBC, JMS, JNDI, porty, certyfikaty i historia zmian.

KIEDY REAGOWAĆ

Brakuje danych potrzebnych do bezpiecznej zmiany lub odtworzenia konfiguracji. Dokumentacja różni się z produkcją.

05-08 / ZASOBY I ZMIANY

Czy masz kontrolę nad zmianami?

Tak = sygnał występuje. Nie wiem = wymaga sprawdzenia.

05

JDBC

Brakuje połączeń w puli

Przy obciążeniu występują timeouty pobierania połączeń, narasta liczba oczekujących albo pula stale osiąga limit.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Zestaw liczbę aktywnych i oczekujących połączeń, czas pobrania, transakcje oraz dostępne zasoby bazy.

KIEDY REAGOWAĆ

Oczekiwanie powoduje timeouty lub narusza cele usługi. Krótki wait sam w sobie nie oznacza awarii; nie zwiększaj puli w ciemno.

06

WSPARCIE

Brak potwierdzonej ścieżki aktualizacji

Nie potrafisz potwierdzić dostępu do poprawek bezpieczeństwa dla używanego serwera, JDK lub systemu.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Zapisz wersję serwera, dostawcę JDK, poprawki i zakres wsparcia. Zweryfikuj dostęp do aktualizacji oraz zgodność wersji.

KIEDY REAGOWAĆ

Brak potwierdzonej ścieżki poprawek bezpieczeństwa. Koniec Premier Support lub sama Java 8 nie przesądzają o braku wsparcia.

07

MONITORING

0 awarii dowiadujesz się od użytkowników

Nie ma alertów związanych z jakością usługi albo brakuje danych JVM, puli połączeń i zależności.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Sprawdź opóźnienia, błędy i dostępność usługi oraz JVM, JDBC i kolejki. Przetestuj alarm i przekazanie go do dyżurnego.

KIEDY REAGOWAĆ

Awaria może pozostać niezauważona albo alert nie trafia do osoby reagującej. Brakuje metryk do diagnozy.

08

WDROŻENIA

Zmian nie można bezpiecznie wycofać

Wdrożenie zależy od ręcznych kroków, a plan powrotu i testy po zmianie są niepełne lub niesprawdzone.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Przejdź ostatnie wdrożenie: artefakt, konfiguracja, zmiany danych i test usługi. Sprawdź plan powrotu oraz czas jego realizacji.

KIEDY REAGOWAĆ

Nie ma przetestowanego powrotu zgodnego z celami usługi. Cofnięcie aplikacji nie musi odwrócić zmian danych.

09-12 / OCHRONA I CIĄGŁOŚĆ

Czy jesteś gotowy na incydent?

Tak = sygnał występuje. Nie wiem = wymaga sprawdzenia.

09 TLS

Certyfikaty nie mają właściciela

Nie ma pełnego rejestru certyfikatów i alarmów o wygaśnięciu albo odnowienie nie było testowane.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Sprawdź rejestr, keystore i truststore oraz certyfikaty na działających endpointach, także za load balancerem.

KIEDY REAGOWAĆ

Czas do wygaśnięcia jest krótszy niż czas bezpiecznej wymiany lub nie ma właściciela. Ustal np. alerty 30/14/7 dni.

10 INCYDENTY

Awaria zamknięta bez wyjaśnienia

Po przywróceniu usługi nie ma analizy przyczyny źródłowej (RCA) ani sprawdzonego działania naprawczego.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Otwórz ostatnie RCA: oś czasu, fakty, hipotezy, przyczyna oraz działania z właścicielem i terminem weryfikacji.

KIEDY REAGOWAĆ

Przyczyna pozostaje niejasna lub działania nie są weryfikowane, a objaw powraca. Sam restart nie zamyka analizy.

11 BEZPIECZEŃSTWO

Hardening i poprawki nie są weryfikowane

Przegląd wykazuje zaległe poprawki, zbędne uprawnienia lub nieuzasadniony dostęp do interfejsów administracyjnych.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Porównaj poprawki i ustawienia z zaleceniami dla danej wersji. Sprawdź dostęp admina, role, TLS oraz wyjątki od polityki.

KIEDY REAGOWAĆ

Podatność i ekspozycja tworzą istotne ryzyko albo wyjątek nie ma właściciela. Sam wiek poprawki nie określa pilności.

12 CIĄGŁOŚĆ

Brak sprawdzonego zastępstwa i odtworzenia

Tylko jedna osoba umie obsłużyć środowisko albo nikt nie potwierdził, że kopie pozwalają odtworzyć usługę.

☐ Tak ☐ Nie ☐ Nie wiem

JAK SPRAWDZIĆ

Niech zastępca wykona test z runbooka poza produkcją. Zweryfikuj kopie, klucze, zależności oraz czas i kompletność odtworzenia.

KIEDY REAGOWAĆ

Zastępca nie potrafi wykonać procedury lub odtworzenie nie spełnia uzgodnionych RTO/RPO (czas / utrata danych).

OD OBSERWACJI DO DECYZJI

Wynik i następny krok

TAK: ____ / 12

NIE WIEM: ____ / 12

0-2 Tak / Pojedyncze sygnały do weryfikacji. Sprawdź każdy z nich.**3-5 Tak / Zaplanuj audyt.** Zacznij od usług o największym wpływie.**6-12 Tak / Priorytetowy przegląd.** Uzgodnij plan stabilizacji.

To orientacyjne progi FlexNet, a nie pomiar ryzyka. Niski wynik nie potwierdza bezpieczeństwa. Odpowiedzi „Nie wiem” wyjaśnij; nie traktuj ich jak „Nie”.

Reaguj niezależnie od wyniku: trwająca awaria, podejrzenie naruszenia lub krytyczna podatność z realną ekspozycją wymagają obsługi incydentowej.

Trzy działania po przeglądzie

SYGNAŁ / DOWÓD / DZIAŁANIE

WŁAŚCICIEL / TERMIN

1.		
2.		
3.		

Jak wygląda Audyt Middleware

01 / ROZMOWA

Ustalamy objawy, zakres i wycenę podczas rozmowy z inżynierem.

02 / MATERIAŁY

Uzgadniamy bezpieczny sposób przekazania potrzebnych logów i konfiguracji.

03 / ANALIZA

Sprawdzamy JVM, zasoby, ustawienia i ryzyka. Weryfikujemy przyczyny objawów.

04 / RAPORT

Dostajesz priorytety, zalecenia i plan działań z szacunkiem nakładu prac.

Omów wynik z inżynierem FlexNet

Podaj numery sygnałów i wpływ na usługę. Audyt jest usługą płatną; zakres i wycenę ustalamy po rozmowie wstępnej.

biuro@flexnet.pl / 606 464 264 / flexnet.pl

Logi i zrzuty mogą zawierać dane poufne. Nie dołączaj ich do pierwszego e-maila; wcześniej uzgodnij zakres i bezpieczny kanał przekazania.

DOKUMENTACJA / KLIKNIJ TYTUŁ

[Oracle / WebLogic: Performance Tuning](#)[Oracle / Java SE Support Roadmap](#)[Oracle / jcmd: wpływ diagnostyki na JVM](#)[IBM / WebSphere Performance Cookbook](#)[IBM / Product Lifecycle](#)[OpenJ9 / jcmd: polecenia diagnostyczne](#)

Materiał pomocniczy; nie zastępuje audytu. © FlexNet 2026 / v20260912-8