Przewodnik po projektowaniu architektury odzyskiwania po awarii (DR)

2020 SOFTPROM *softprom.com* | *info@softprom.com* **Amazon Web Services Partner Network ADVANCED CONSULTING PARTNER** —

Projektowanie architektury Disaster Recovery (DR) w AWS

Projektowanie architektury odzyskiwania po awarii (DR) może mieć zastosowanie zarówno w środowisku hybrydowym, gdzie główne moce produkcyjne znajdują się w lokalnym centrum danych (on-premise), a w chmurze przechowywane są kopie zapasowe, obrazy do szybkiego wdrożenia lub gotowe do uruchomienia bądź współdzielące obciążenie zapasowe infrastruktury. Rozwiązanie to ma również zastosowanie dla infrastruktury działającej w całości w chmurze AWS, posiadającej redundancję w różnych regionach AWS. Koszt wdrożenia poszczególnych modeli jest również istotnym czynnikiem przy wyborze odpowiedniej strategii.

Ciągłość działania biznesu (Business Continuity)

Czynnikami decydującymi o wyborze i projektowaniu architektury DR są parametry wymagane przez biznes: RPO (punkt przywracania) oraz RTO (czas przywracania).

- **RPO (Recovery Point Objective):** Odpowiada na pytanie, na utratę lub ponowne odtworzenie jakiej ilości danych biznes może sobie pozwolić. Mierzy potencjalną utratę danych (*Data loss*) od momentu awarii wstecz.
- **RTO (Recovery Time Objective):** Odpowiada na pytanie, jak szybko należy przywrócić działanie środowiska oraz jaki jest koszt przestoju. Mierzy czas przestoju (*Down time*) od momentu wystąpienia awarii do pełnego przywrócenia usług.

Scenariusze odzyskiwania po awarii (DR) w AWS

Wybór konkretnego scenariusza DR zależy od priorytetów biznesowych, wymaganych parametrów RTO/RPO oraz kosztów wdrożenia danej opcji. W AWS można wyróżnić cztery podstawowe scenariusze:

1. Kopie zapasowe i odtwarzanie (Backup & Restore)

- **Parametry RPO/RTO:** Liczone w godzinach.
- **Priorytet:** Przeznaczony dla mniej krytycznych przypadków użycia (*Lower priority use cases*).
- **Rozwiązania:** AWS S3, Elastic Block Store (EBS).
- **Koszt:** Najniższy ($).
- **Charakterystyka:** Dane krytyczne dla biznesu mogą być regularnie backupowane do pamięci obiektowej AWS S3. Zapewnia to bezpieczne i niezawodne przechowywanie kopii zapasowych oraz pozwala na ich szybkie pobranie w celu odtworzenia działającej infrastruktury.
- **Integracja On-Premise:** Do zapisu lokalnych kopii zapasowych w AWS wykorzystywana jest usługa *AWS Storage Gateway* w 3 opcjach:
    - *File Gateway* (dostęp przez NFS v3 / v4.1 do S3 Standard, S3-IA, Glacier).
    - *Volume Gateway* (dostęp przez iSCSI do S3 i tworzenie migawek EBS Snapshots).
    - *Tape Gateway VTL* (dostęp przez VTL-iSCSI do przechowywania wirtualnych taśm w S3 i Glacier).

2. Środowisko Pilotowe (Pilot Light)

- **Parametry RPO/RTO:** Liczone w minutach.
- **Priorytet:** Spełnienie niższych wymagań RTO i RPO dla usług rdzeniowych (*Core services*).
- **Koszt:** Niski ($$).
- **Charakterystyka:** W chmurze wdrożony jest wyłączony, “zamrożony” i zmniejszony odpowiednik środowiska produkcyjnego. Należy stale dbać o aktualność tej zapasowej infrastruktury. Najważniejsze komponenty można szybko uruchomić w AWS przy użyciu przygotowanych obrazów Amazon Machine Images (AMI) oraz migawek Amazon EBS Snapshots. Metoda ta znacznie skraca czas przywracania w porównaniu do tradycyjnego Backup & Restore.

3. Ciepła rezerwa (Warm Standby)

- **Parametry RPO/RTO:** Liczone w sekundach lub minutach.
- **Priorytet:** Przeznaczone dla usług krytycznych dla biznesu (*Business critical services*).

- **Koszt:** Średni ($).
- **Charakterystyka:** W chmurze AWS stale działa mniejsza, skalowalna wersja głównej infrastruktury produkcyjnej (*Scaled down standby*). Baza danych podlega ciągłej replikacji i mirroringowi. W przypadku awarii ruch produkcyjny jest przełączany (np. za pomocą Route 53 i Elastic Load Balancera), a infrastruktura w chmurze jest błyskawicznie skalowana w górę (*Scaled-up production*), aby obsłużyć pełne obciążenie i zminimalizować czas przestoju.

4. Wdrożenie wieloobiektowe / Aktywna rezerwa (Multi-site deployment / "Hot Standby")

- **Parametry RPO/RTO:** W czasie rzeczywistym (*Real-time*).
- **Priorytet:** Wysoki priorytet z automatycznym przełączaniem awaryjnym (*Auto-failover*).
- **Koszt:** Najwyższy ($$).
- **Charakterystyka:** Pełna infrastruktura produkcyjna jest równolegle zainstalowana w kilku miejscach jednocześnie — na przykład w lokalnym centrum danych i w AWS lub w różnych regionach AWS. Wszystkie te klony środowiska są stale aktywne, dzielą między sobą ruch oraz obciążenie, a dane i kluczowe komponenty są nieustannie replikowane. W razie awarii jednego z miejsc, pozostała działająca część infrastruktury przejmuje całe obciążenie bez przerywania pracy. Do realizacji tego scenariusza wykorzystuje się m.in. *Amazon EC2 Auto Scaling*. Dzięki jednoczesnej pracy wielu wirtualnych infrastruktur parametry RTO/RPO są minimalne.

Kluczowe funkcje i pojęcia Disaster Recovery

- **Replikacja (Replication):** W celu zapewnienia wysokiej dostępności wdraża się replikację między różnymi regionami AWS. Krytyczne dane i komponenty systemowe są kopiowane do innego wybranego regionu. Zmiany w głównej bazie danych mogą być odświeżane natychstowo (replikacja synchroniczna) lub z niewielkim opóźnieniem (replikacja asynchroniczna), w zależności od potrzeb biznesu.
- **Powrót do stanu pierwotnego (Failback):** Podczas awarii obciążenie zostaje przeniesione na zapasową instancję infrastruktury. Po naprawieniu i przywróceniu pierwotnej instancji można zsynchronizować dane (kierując replikację z instancji zapasowej na główną) i przywrócić jej najwyższy priorytet.
- **Wiele regionów AWS (Multiple AWS regions):** Każdy region AWS stanowi całkowicie oddzielny i niezależny obszar geograficzny. Przechowywanie danych w

dwóch lub więcej regionach pozwala całkowicie wyeliminować skutki katastrof o charakterze wielkoskalowym.

Najlepsze praktyki odzyskiwania po awarii w AWS

- **Testowanie (Testing):** Po wdrożeniu rozwiązania DR należy je regularnie testować na żądanie lub według harmonogramu. Pozwala to sprawdzić realizację założeń RTO/RPO. Do automatycznego wdrażania potrzebnych środowisk w Amazon EC2 warto używać *AWS CloudFormation*. Szablony pozwalają modelować komponenty infrastruktury i zarządzać nimi. Cykliczne testy dają pewność, że plan zadziała w krytycznym momencie.
- **Monitorowanie i alerty (Monitoring and alerting):** Niezbędne jest ciągłe monitorowanie w celu wczesnego wykrywania zagrożeń i szybkiej reakcji. System *Amazon CloudWatch* pozwala śledzić wszystkie zdarzenia w infrastrukturze chmurowej oraz konfigurować alerty i powiadomienia, gdy wskaźniki osiągną poziomy krytyczne.
- **Regularny backup i replikacja (Regular backup and replication):** Regularne tworzenie kopii zapasowych jest kluczowe dla posiadania aktualnych danych do przełączenia awaryjnego. Po przełączeniu na infrastrukturę DR procesy backupu i replikacji powinny być kontynuowane. Przechowywanie kopii w odizolowanych, odległych lokalizacjach eliminuje ryzyko pojedynczego punktu awarii (*single point of failure*). AWS pozwala także uruchamiać automatyczne testy sprawdzające stan infrastruktury DR.
- **Wykorzystanie narzędzi i technik AWS (Use of AWS tools and techniques):** Należy wdrażać dedykowane grupy odzyskiwania lub stosy aplikacji. Pozwala to odpowiednio zorganizować proces i zapewnić, że aplikacje o najwyższym priorytecie dla biznesu zostaną odtworzone w pierwszej kolejności.

---

10 porad przy tworzeniu planu Disaster Recovery w AWS

1. Przechowuj kopie zapasowe wolumenów AWS EBS w różnych strefach dostępności (AZ) lub regionach AWS.
2. Stosuj wdrożenia wielostrefowe (Multi-AZ) dla instancji AWS EC2 oraz baz danych RDS.
3. Rozmieszczaj dane w AWS S3 w różnych regionach i dbaj o ich synchronizację.
4. W bazach AWS DynamoDB używaj replikacji danych pomiędzy różnymi regionami AWS.

5. Podejdź odpowiedzialnie do ochrony poświadczeń konta głównego (*AWS Root Credentials*) — bezwzględnie włącz MFA na koncie root.
6. Jasno zdefiniuj parametry RTO oraz RPO dla swojego biznesu.
7. Wybierz właściwy plan/scenariusz odzyskiwania po awarii dostosowany do potrzeb.
8. Zidentyfikuj aplikacje krytyczne dla działania firmy i opracuj dla nich dedykowany plan DR.
9. Regularnie testuj swoją implementację mechanizmów odzyskiwania po awarii.
10. W celu zwiększenia elastyczności rozważ użycie rozwiązań firm zewnętrznych (*third-party*) w obszarze Disaster Recovery (DR).