Odporne architektury, część 2: RDS Multi-AZ, Aurora, AWS Backup i strategie DR

Poziom: średnio

Dotyczy: SAA-C03 domena 2, zadanie 2.2 (wysoka dostępność i odporność na awarie) oraz część zadań 1.3 i 3.3, Amazon RDS, Amazon Aurora, RDS Proxy, AWS Backup, AWS Elastic Disaster Recovery, replikacja S3, dni 15 do 17 planu

Czas: 3 dni po 1,5 do 2 godzin

Aplikacja bezstanowa przeżyje awarię strefy, jeśli przeżyją ją dane. Ta strona opisuje bazy RDS w trybie Multi-AZ i z replikami odczytu, Aurorę, kopie zapasowe w AWS Backup i cztery strategie odtwarzania po katastrofie z ich czasami RTO i RPO. Na egzaminie te słowa pojawiają się w co drugim pytaniu z tej domeny.

ZAŁOŻENIA SCENARIUSZA

ćwiczenia robimy w VPC laboratorium 10.60.0.0/16, a bazy stoją w podsieciach `db-a`, `db-b` i `db-c`. Region zapasowy w projekcie sklepu to `eu-west-1` (Irlandia); w laboratorium SCP `tylko-frankfurt` go blokuje, więc kopie między regionami opisujemy, a w laboratorium robimy tylko kopie w obrębie Frankfurtu. Pojęcia RPO i RTO w Zielonej opisuje strona Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje.

Skróty użyte na tej stronie (23)

Skrót	Co znaczy
ACU	Aurora Capacity Unit: jednostka mocy Aurora Serverless, w której baza rośnie i maleje według obciążenia
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
AWS	Amazon Web Services: chmura Amazonu
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
CRR	Cross-Region Replication: replikacja obiektów S3 do kubełka w innym regionie

Skrót	Co znaczy
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DR	Disaster Recovery: plan przywrócenia działania po poważnej awarii
DynamoDB	baza danych typu klucz-wartość w chmurze AWS; Lore trzyma w niej fragmenty, stan, magazyn zmienny i blokady, gdy działa na AWS
EBS	Elastic Block Store: dyski blokowe maszyn wirtualnych EC2 w chmurze AWS, rozliczane osobno od maszyny
EC2	Elastic Compute Cloud: usługa AWS wynajmująca gotowe maszyny wirtualne na godziny
EFS	Elastic File System: współdzielony system plików NFS w AWS, dostępny z wielu instancji i stref
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
KMS	Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi
PITR	Point-In-Time Recovery: odtworzenie bazy do dowolnej chwili, np. 14:31
RDS	Remote Desktop Services: zdalne pulpity i aplikacje Windows Server
RPO	Recovery Point Objective: ile danych wolno stracić przy awarii
RTO	Recovery Time Objective: jak długo wolno nie działać przy awarii
S3	Simple Storage Service: magazyn plików w chmurze AWS
SAA-C03	kod wersji egzaminu AWS Solutions Architect Associate zdawanej od 30 sierpnia 2022, aktualnej w październiku 2026
SCP	Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym
TiB	tebibajt: 2 do potęgi 40 bajtów, jednostka, w której liczą Windows i PowerShell (1TB w PowerShellu); dysk z etykietą 2 TB ma około 1,82 TiB
UTC	Coordinated Universal Time: uniwersalny czas bez strefy, punkt odniesienia dla wszystkich stref czasowych na świecie
VPC	Virtual Private Cloud: prywatna sieć wirtualna klienta w chmurze AWS, w której stawiamy maszyny i zakładamy tablice tras

Fiszka

Komendy wykonujemy w CloudShell z profilem konta laboratorium. `NazwaInstancji`, `NazwaKlastra`, `IdGrupyDb`, `NazwaSejfu`, `IdPlanu` i podobne zastępujemy własnymi. Instancje baz są płatne za godzinę, także zatrzymane po siedmiu dniach same się uruchamiają, więc usuwamy je w dniu ćwiczenia.

ZMIENIA SYSTEM

Utworzenie grupy podsieci dla bazy: aws rds create-db-subnet-group

```
aws rds create-db-subnet-group --db-subnet-group-name lab-db --db-subnet-group-description "Podsieci baz laboratorium" --subnet-ids IdPodsieciDbA IdPodsieciDbB IdPodsieciDbC
```

RDS wybiera z tej grupy podsieć dla instancji głównej i zapasowej. Grupa musi obejmować co najmniej dwie strefy.

RDS = Remote Desktop Services: zdalne pulpity i aplikacje Windows Server · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie bazy MariaDB w trybie Multi-AZ: aws rds create-db-instance --multi-az

```
aws rds create-db-instance --db-instance-identifier lab-sklep --engine mariadb --db-instance-class db.t4g.micro --allocated-storage 20 --storage-type gp3 --master-username admin_sklep --manage-master-user-password --multi-az --db-subnet-group-name lab-db --vpc-security-group-ids IdGrupyDb --no-publicly-accessible --storage-encrypted --kms-key-id alias/lab-dane --backup-retention-period 7
```

`--manage-master-user-password` zapisuje hasło administratora w Secrets Manager zamiast w poleceniu. `--multi-az` dokłada synchroniczną instancję zapasową w innej strefie, do której nie da się podłączyć, dopóki nie nastąpi przełączenie. Dostępność klasy `db.t4g.micro` w trybie Multi-AZ dla danej wersji silnika sprawdzamy w konsoli przy tworzeniu.

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Wymuszenie przełączenia na instancję zapasową: aws rds reboot-db-instance --force-failover

```
aws rds reboot-db-instance --db-instance-identifier lab-sklep --force-failover
aws rds describe-events --source-identifier lab-sklep --source-type db-instance --duration 30
```

Restart z przełączeniem to próba awarii strefy. Adres końcowy bazy się nie zmienia, zmienia się tylko adres IP za nim, więc aplikacja z krótkim czasem pamięci DNS łączy się ponownie sama.

IP = Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection) · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie repliki odczytu: aws rds create-db-instance-read-replica

```
aws rds create-db-instance-read-replica --db-instance-identifier lab-sklep-odczyt --source-db-instance-identifier lab-sklep
```

Replika dostaje dane asynchronicznie, ma własny adres i przyjmuje tylko odczyty. Może stać w innym regionie, a w razie potrzeby można ją awansować na samodzielną bazę poleceniem `aws rds promote-read-replica --db-instance-identifier lab-sklep-odczyt`.

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Odtworzenie bazy na wybraną chwilę: aws rds restore-db-instance-to-point-in-time

```
aws rds restore-db-instance-to-point-in-time --source-db-instance-identifier lab-sklep --target-db-instance-identifier lab-sklep-odtw --restore-time 2026-10-19T09:15:00Z --db-subnet-group-name lab-db --vpc-security-group-ids IdGrupyDb
```

Odtworzenie zawsze tworzy nową instancję z nowym adresem. Zamiast `--restore-time` można podać `--use-latest-restorable-time`. Najpóźniejszy możliwy czas pokazuje pole `LatestRestorableTime` w `describe-db-instances`.

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Ręczna migawka bazy: aws rds create-db-snapshot

```
aws rds create-db-snapshot --db-instance-identifier lab-sklep --db-snapshot-identifier
lab-sklep-przed-zmiana
```

Kopie automatyczne znikają razem z okresem przechowywania (do 35 dni) i domyślnie przy usunięciu instancji, a migawka ręczna zostaje, dopóki jej nie usuniemy.

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie klastra Aurora MySQL z instancją zapisującą: aws rds create-db-cluster

```
aws rds create-db-cluster --db-cluster-identifier lab-aurora --engine aurora-mysql --
master-username admin_sklep --manage-master-user-password --db-subnet-group-name lab-db
--vpc-security-group-ids IdGrupyDb --storage-encrypted
aws rds create-db-instance --db-instance-identifier lab-aurora-1 --db-cluster-identifier
lab-aurora --engine aurora-mysql --db-instance-class db.t4g.medium
```

Klaster Aurora to wspólny wolumen danych i instancje, które z niego korzystają. Druga instancja w innej strefie (to samo polecenie z inną nazwą) staje się repliką, na którą klaster przełącza się przy awarii.

aws = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Przełączenie klastra Aurora: aws rds failover-db-cluster

```
aws rds failover-db-cluster --db-cluster-identifier lab-aurora
```

Adres zapisu klastra zaczyna wskazywać awansowaną replikę. Bez repliki Aurora tworzy nową instancję, co trwa dłużej.

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie sejfu kopii: aws backup create-backup-vault

```
aws backup create-backup-vault --backup-vault-name lab-sejf --encryption-key-arn ArnKluczaKms
```

Sejf to kontener na punkty odtworzenia, szyfrowany kluczem KMS i z własną polityką dostępu.

KMS = Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi · **aws** = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Zablokowanie sejfu przed skróceniem retencji: aws backup put-backup-vault-lock-configuration

```
aws backup put-backup-vault-lock-configuration --backup-vault-name lab-sejf --min-retention-days 7 --max-retention-days 35 --changeable-for-days 3
```

Przez trzy dni blokadę można jeszcze usunąć (tryb zarządzania), potem staje się nieodwracalna (tryb zgodności) i nikt, także użytkownik główny, nie usunie kopii przed czasem. W laboratorium pomijamy `--changeable-for-days`, żeby blokada została w trybie zarządzania i dała się usunąć.

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie planu kopii: aws backup create-backup-plan

```
aws backup create-backup-plan --backup-plan file://plan-kopii.json
```

aws = AWS CLI: narzędzie chmury Amazonu

PLIK KONFIGURACYJNY

Plan codziennej kopii z kopią do drugiego regionu: plan-kopii.json

```
{
  "BackupPlanName": "sklep-codziennie",
  "Rules": [
    {
```

```
      "RuleName": "codziennie-0100",
      "TargetBackupVaultName": "lab-sejf",
      "ScheduleExpression": "cron(0 1 * * ? *)",
      "StartWindowMinutes": 60,
      "Lifecycle": { "DeleteAfterDays": 35 },
      "CopyActions": [
        {
          "DestinationBackupVaultArn": "arn:aws:backup:eu-west-1:IdKonta:backup-
vault:sejf-irlandia",
          "Lifecycle": { "DeleteAfterDays": 35 }
        }
      ]
    }
  ]
}
```

Wyrażenie `cron` w AWS ma sześć pól (z rokiem) i liczy czas w UTC. W laboratorium usuwamy blok `CopyActions`, bo SCP blokuje `eu-west-1`.

AWS = Amazon Web Services: chmura Amazonu · **UTC** = Coordinated Universal Time: uniwersalny czas bez strefy, punkt odniesienia dla wszystkich stref czasowych na świecie · **SCP** = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym

ZMIENIA SYSTEM

Wskazanie zasobów do kopii po tagu: aws backup create-backup-selection

```
aws backup create-backup-selection --backup-plan-id IdPlanu --backup-selection
file://wybor-kopii.json
```

aws = AWS CLI: narzędzie chmury Amazonu

PLIK KONFIGURACYJNY

Wybór zasobów po tagu: wybor-kopii.json

```
{
  "SelectionName": "tag-kopia-codziennie",
```

```
  "IamRoleArn": "arn:aws:iam::IdKonta:role/service-role/AWSBackupDefaultServiceRole",
  "ListOfTags": [
    { "ConditionType": "STRINGEQUALS", "ConditionKey": "kopia", "ConditionValue":
"codziennie" }
  ]
}
```

Każdy zasób z tagiem `kopia=codziennie` (baza, dysk EBS, system plików EFS, tabela DynamoDB) trafia do planu bez zmiany planu. Rola domyślna powstaje przy pierwszym użyciu AWS Backup w konsoli, a jej istnienie sprawdzamy przed wywołaniem.

EBS = Elastic Block Store: dyski blokowe maszyn wirtualnych EC2 w chmurze AWS, rozliczane osobno od maszyny · **EFS** = Elastic File System: współdzielony system plików NFS w AWS, dostępny z wielu instancji i stref · **DynamoDB** = baza danych typu klucz-wartość w chmurze AWS; Lore trzyma w niej fragmenty, stan, magazyn zmienny i blokady, gdy działa na AWS · **AWS** = Amazon Web Services: chmura Amazonu

TYLKO ODCZYT

Lista punktów odtworzenia w sejfie: aws backup list-recovery-points-by-backup-vault

```
aws backup list-recovery-points-by-backup-vault --backup-vault-name lab-sejf --query
"RecoveryPoints[].[ResourceType,CreationDate,Status]" --output table
```

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Włączenie odtwarzania na chwilę dla tabeli DynamoDB: aws dynamodb update-continuous-backups

```
aws dynamodb update-continuous-backups --table-name NazwaTabeli --point-in-time-
recovery-specification PointInTimeRecoveryEnabled=true
```

Tabelę można potem odtworzyć do dowolnej sekundy z okresu przechowywania, domyślnie 35 dni, do nowej tabeli.

DynamoDB = baza danych typu klucz-wartość w chmurze AWS; Lore trzyma w niej fragmenty, stan, magazyn zmienny i blokady, gdy działa na AWS · **aws** = AWS CLI: narzędzie chmury Amazonu

Z życia wzięte

Z ŻYCIA WZIĘTE

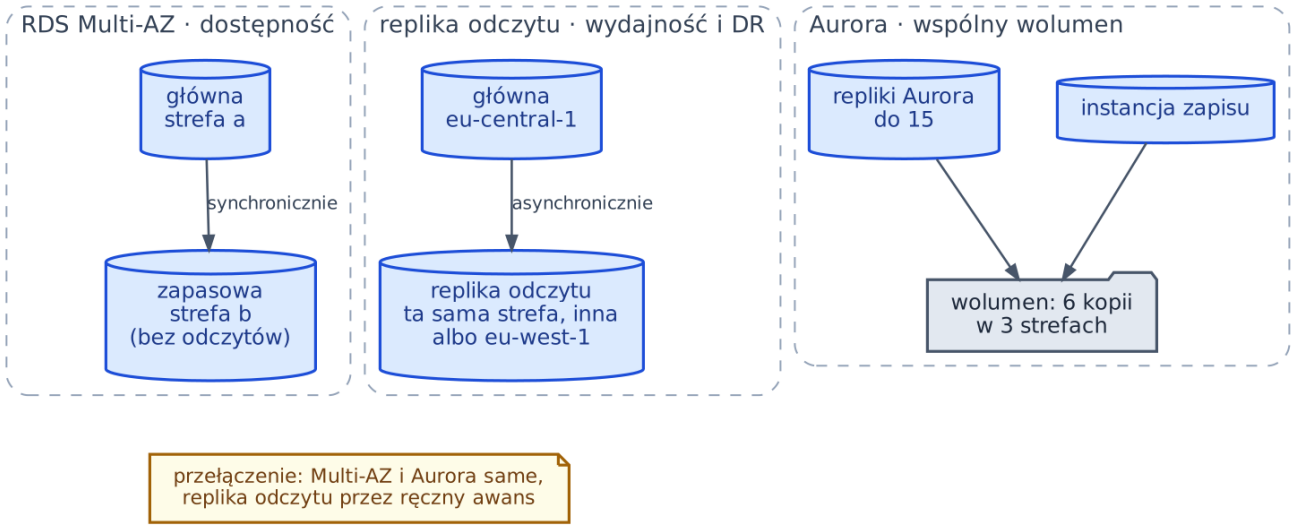
Czwartek, 11:45. Tomek pokazuje Kasi bazę sklepu w laboratorium z repliką odczytu w innej strefie i mówi, że to jest wysoka dostępność. Ola pyta, co się stanie, gdy w nocy padnie strefa z bazą główną, a nikt nie będzie przy komputerze. Tomek sprawdza w dokumentacji i odkrywa, że replika odczytu sama się nie awansuje, a Multi-AZ przełącza się bez nas. W projekcie zostają oba: Multi-AZ na awarię strefy, replika odczytu dla raportów Kasi.

Jak to działa

Rozwiń: jak to działa pod spodem

RDS: Multi-AZ i repliki odczytu

Multi-AZ służy dostępności, a repliki odczytu wydajności. To najczęstsze rozróżnienie w tej domenie i warto je mieć jako jedno zdanie w dzienniku.



Rysunek 1. Trzy sposoby odporności bazy: RDS Multi-AZ z synchroniczną instancją zapasową, repliki odczytu z asynchroniczną kopią, także w innym regionie, i Aurora ze wspólnym wolumenem w trzech strefach (kliknięcie otwiera pełny rozmiar)

Cecha	RDS Multi-AZ (instancja)	RDS Multi-AZ (klaster, dwie zapasowe)	Replika odczytu	Aurora
Cel	dostępność	dostępność i odczyty	odczyty, kopia w innym regionie	dostępność, odczyty, wydajność
Replikacja	synchroniczna	półsynchroniczna	asynchroniczna	wspólny wolumen, sześć kopii w trzech strefach
Odczyt z kopii	nie	tak	tak	tak, do 15 replik
Przełączenie	automatyczne, ten sam adres	automatyczne	ręczne awansowanie	automatyczne, adres zapisu klastra
Inny region	nie	nie	tak	Aurora Global Database
Silniki	wszystkie RDS	MySQL i PostgreSQL	większość silników	Aurora MySQL i Aurora PostgreSQL

Czasy przełączenia podajemy z dokumentacji jako rzędy wielkości: Multi-AZ instancji to zwykle jedna do dwóch minut, Aurora z repliką zwykle poniżej minuty. Na egzaminie liczy się porównanie, a nie dokładna liczba.

> **Pojęcie: RDS Proxy.** Zarządzana pula połączeń przed bazą RDS albo Aurora. Przydaje się, gdy wiele krótkich połączeń (funkcje Lambda) zabija bazę liczbą sesji, i skraca przełączenie, bo aplikacja rozmawia z proxy, a nie z adresem bazy.

> **Pojęcie: Aurora Serverless v2.** Tryb Aurory, w którym moc instancji rośnie i maleje sama w jednostkach ACU, według obciążenia. Dobry dla zmiennego albo nieprzewidywalnego ruchu.

Aurora rośnie sama do 256 TiB (od lipca 2025 roku dla nowszych wersji silników, wcześniej 128 TiB, starsze materiały podają tę drugą liczbę). Aurora Global Database replikuje do innych regionów z opóźnieniem typowo poniżej sekundy, a przełączenie regionu trwa według AWS około minuty.

Kopie zapasowe w AWS

Co	Mechanizm	Uwagi
RDS i Aurora	kopie automatyczne z odtwarzaniem na chwilę (1 do 35 dni) i migawki ręczne	odtwarzanie tworzy nową instancję
EBS	migawki przyrostowe w S3	kopia do innego regionu, Data Lifecycle Manager do harmonogramu
S3	wersjonowanie, replikacja w regionie (SRR) i między regionami (CRR), Object Lock	replikacja wymaga wersjonowania po obu stronach i nie kopiuje wstecz obiektów sprzed jej włączenia bez Batch Replication
DynamoDB	odtwarzanie na chwilę (PITR) i kopie na żądanie	odtworzenie do nowej tabeli
EFS, FSx	AWS Backup	
Wszystko naraz	AWS Backup: plany, sejfy, blokada sejfu, kopie między kontami i regionami	jedno miejsce na politykę kopii i raport dla audytora
Całe serwery z serwerowni	AWS Elastic Disaster Recovery	ciągła replikacja dysków, uruchomienie w AWS w minutach

Strategie odtwarzania po katastrofie

Pojęcie: RPO (Recovery Point Objective). Ile danych, liczonych w czasie, możemy stracić. RPO 5 minut oznacza, że po katastrofie brakuje najwyżej ostatnich pięciu minut.

Pojęcie: RTO (Recovery Time Objective). Jak długo system może nie działać, od awarii do przywrócenia.



Rysunek 2. Cztery strategie DR od najtańszej do najdroższej: kopia i odtworzenie, pilot light, ciepła rezerwa i aktywne w wielu miejscach, z typowymi RTO i RPO (kliknięcie otwiera pełny rozmiar)

Strategia	Co działa w regionie zapasowym	Typowe RTO i RPO	Koszt
kopia i odtworzenie (backup and restore)	tylko kopie	godziny	najniższy
pilot light	dane replikowane na bieżąco, serwery wyłączone albo w szablonie	dziesiątki minut, RPO minuty	niski
ciepła rezerwa (warm standby)	pomniejszona, działająca kopia całego systemu	minuty	średni
aktywne w wielu miejscach (multi-site active/active)	pełny system przyjmujący ruch	bliskie zera	najwyższy

Typowe wartości to rzędy wielkości z dokumentacji AWS o DR, a nie gwarancje. W pytaniu szukamy najtańszej strategii, która spełnia podane RTO i RPO.

Pułapki egzaminacyjne

- „Wysoka dostępność bazy” albo „awaria strefy”: Multi-AZ. Replika odczytu jest odpowiedzią na „raporty spowalniają bazę”.
- Replika odczytu w innym regionie to dobry element strategii DR, ale bez awansowania nie przyjmie zapisów.
- RPO w sekundach i RTO w minutach dla bazy w wielu regionach: Aurora Global Database (albo DynamoDB global tables dla NoSQL).

- Wiele funkcji Lambda wyczerpuje połączenia do bazy: RDS Proxy.
- Szyfrowanie istniejącej bazy: migawka, kopia migawki z szyfrowaniem, odtworzenie. Replika odczytu nie zaszyfruje się sama, jeśli źródło nie jest szyfrowane.
- Kopie mają być nieusuwalne nawet przez administratora: AWS Backup Vault Lock w trybie zgodności albo S3 Object Lock w trybie zgodności.
- Stary system z serwerowni ma mieć DR w AWS bez przepisywania: AWS Elastic Disaster Recovery.
- Przy usunięciu instancji RDS kopie automatyczne domyślnie znikają; migawkę końcową trzeba zrobić albo zachować kopie automatyczne.

Częste błędy

Objaw	Przyczyna	Co robimy
Aplikacja po przełączeniu Multi-AZ łączy się dalej ze starym adresem IP	pamięć DNS w aplikacji albo w JVM	krótki czas pamięci DNS, ponowne łączenie w kodzie, RDS Proxy
Nie da się wybrać `--multi-az` dla klasy instancji	ta klasa albo wersja silnika nie obsługuje Multi-AZ w regionie	inna klasa, sprawdzenie w konsoli
Odtworzona baza nie ma tych samych grup i parametrów	odtworzenie tworzy nową instancję z domyślnymi ustawieniami	podajemy grupę podsieci, grupy zabezpieczeń i grupę parametrów w poleceniu
Plan AWS Backup nie robi kopii	zasób nie ma tagu albo rola nie ma uprawnień	tag `kopia=codziennie`, `AWSBackupDefaultServiceRole`
Kopia do drugiego regionu kończy się błędem uprawnień	SCP blokuje region albo klucz KMS w regionie docelowym	wyjątek w SCP dla regionu zapasowego, sejf z kluczem w tamtym regionie
Rachunek za bazę po zakończeniu ćwiczeń	instancja zatrzymana uruchamia się sama po siedmiu dniach	usuwamy instancję z `--skip-final-snapshot` po ćwiczeniu

□□ Ćwiczenia

1. Dzień 15. Tworzymy bazę `lab-sklep` w trybie Multi-AZ, wymuszamy przełączenie i mierzymy, jak długo baza nie przyjmowała połączeń. Jak to zmierzyć z instancji w podsieci aplikacji?

Odpowiedź

Na instancji z klientem MariaDB uruchamiamy pętlę, która co sekundę wypisuje czas i wynik prostego zapytania, a w drugim oknie wymuszamy przełączenie:

```
while true; do printf '%s ' "$(date +%T)"; mysql -h AdresBazy -u admin_sklep -p"$HASLO" -e "select 1" -sN 2>&1 | head -1; sleep 1; done
```

```
aws rds reboot-db-instance --db-instance-identifier lab-sklep --force-failover
```

Liczymy sekundy z błędami połączenia. Hasło pobieramy wcześniej z Secrets Manager do zmiennej `HASLO`. Po ćwiczeniu: `aws rds delete-db-instance --db-instance-identifier lab-sklep --skip-final-snapshot --delete-automated-backups`.

1. Dzień 17. Kasia wymaga dla sklepu RTO 1 godzina i RPO 5 minut przy utracie całego regionu Frankfurt. Która najtańsza strategia DR to spełni i z jakich usług ją zbudujemy?

Odpowiedź

Pilot light: replika odczytu bazy MariaDB w `eu-west-1` (albo Aurora Global Database, jeśli przejdziemy na Aurorę), kubełek zdjęć z replikacją CRR, szablon CloudFormation całej warstwy aplikacji gotowy do uruchomienia, Route 53 z polityką failover. Przy awarii awansujemy replikę, uruchamiamy stos i przełączamy DNS. Replika asynchroniczna daje RPO poniżej pięciu minut przy normalnym opóźnieniu, a uruchomienie stosu i awans mieszczą się w godzinie, co sprawdzamy próbą. Sama kopia i odtworzenie nie da RPO 5 minut, a ciepła rezerwa jest droższa niż potrzeba.

1. Dzień 17. Zakładamy sejf `lab-sejf`, plan `sklep-codziennie` bez kopii do drugiego regionu i wybór po tagu, oznaczamy tagiem dysk EBS i uruchamiamy kopię na żądanie. Jakie polecenie uruchamia kopię od razu?

Odpowiedź

```
aws backup start-backup-job --backup-vault-name lab-sejf --resource-arn arn:aws:ec2:eu-central-1:IdKonta:volume/IdDysku --iam-role-arn arn:aws:iam::IdKonta:role/service-role/AWSBackupDefaultServiceRole
aws backup list-backup-jobs --by-backup-vault-name lab-sejf --query "BackupJobs[].[ResourceType,State]" --output table
```

Punkt odtworzenia pojawia się w `list-recovery-points-by-backup-vault`. Przed usunięciem sejfu trzeba usunąć wszystkie punkty, a sejfu z blokadą w trybie zgodności nie da się wyczyścić przed końcem retencji.

1. Pytanie w stylu egzaminu: aplikacja raportowa wykonuje ciężkie zapytania na produkcyjnej bazie RDS PostgreSQL i spowalnia sklep. Co robimy z najmniejszym wysiłkiem?

Odpowiedź

Replika odczytu RDS i skierowanie aplikacji raportowej na jej adres. Multi-AZ z jedną instancją zapasową nie pomoże, bo instancja zapasowa nie przyjmuje odczytów. ElastiCache też nie jest odpowiedzią przy ciężkich, różnorodnych zapytaniach raportowych.

1. Pytanie w stylu egzaminu: firma potrzebuje relacyjnej bazy z odczytami w trzech regionach o małym opóźnieniu i przełączeniem regionu w około minutę przy RPO rzędu sekundy. Co wybiera?

Odpowiedź

Aurora Global Database z klastrem głównym w jednym regionie i klastrami wtórnymi w dwóch pozostałych. Repliki odczytu RDS między regionami dałyby odczyty, ale nie takie RPO i RTO przy przełączeniu.

Krok projektu: sklep B2B

Baza `sklep_b2b` z `my01` przechodzi do RDS for MariaDB w trybie Multi-AZ w podsieciach `db`, szyfrowana kluczem zarządzanym przez klienta, z kopiami automatycznymi przez 14 dni i repliką odczytu w `eu-west-1` dla strategii pilot light. Katalog z `mongo01` ma dwie drogi do decyzji: Amazon DocumentDB (zgodny z API MongoDB, zarządzany) albo MongoDB na EC2 z własną replikacją, co opisujemy przy wyborze baz na stronie Wydajne architektury: obliczenia, magazyn, bazy, CloudFront i strumienie danych. AWS Backup z planem po tagu kopiuje bazę i dyski do sejfu z blokadą, z kopią do drugiego regionu. Próbę przełączenia regionu robimy raz na kwartał, poza okresem zakazu zmian od 15 listopada do 6 stycznia.

Powiązane: Odporne architektury, część 1: strefy, ELB, Auto Scaling, Route 53 i luźne powiązania · Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje · Replikacja · Zimne archiwum w chmurze: Azure Blob Storage i Amazon S3 Glacier · Azure Site Recovery dla Hyper-V bez VMM: replikacja, test, przełączenie i powrót

Źródła: przewodnik SAA-C03, domena 2, zadanie 2.2; dokumentacja Amazon RDS (Multi-AZ instancji i klastra, repliki odczytu, odtwarzanie na chwilę, RDS Proxy, automatyczne uruchamianie zatrzymanych instancji po siedmiu dniach); dokumentacja Amazon Aurora (wolumen w trzech strefach, Global Database, Serverless v2), komunikaty AWS z lipca 2025 o wolumenach do 256 TiB;

dokumentacja AWS Backup (plany, wybory, Vault Lock); whitepaper AWS „Disaster Recovery of Workloads on AWS” (cztery strategie); dokumentacja DynamoDB (PITR); dokumentacja AWS Elastic Disaster Recovery. Parametry poleceń sprawdzone z modelem usług AWS CLI (botocore 1.43) 19 października 2026.

Revision #4
Created 2026-10-18 23:00:39 UTC by Tomasz Konieczny
Updated 2026-11-01 18:03:24 UTC by Tomasz Konieczny