Recuperação

Recupere o serviço e reconcilie as operações externas

Declare o incidente e contenha novas gravações

Registre o início da interrupção, o impacto e a pessoa que coordena a resposta. Se houver risco de dois bancos aceitarem escritas divergentes, pause as gravações da API e dos workers antes de trocar o destino.

Restaure o conjunto que o serviço usa

Escolha o ponto recuperável e restaure em uma instância separada. Confira esquema, permissões e dados conhecidos. Teste com a versão da API que será usada na retomada e considere também dependências como filas e pagamentos.

Meça a retomada

Registre o último ponto de dados recuperável e o horário em que o serviço passou a aceitar operações válidas. Compare com os objetivos de perda de dados e tempo de recuperação.

Recuperação

Ensaie a volta da agenda em homologação

Sequência do exercício

```
1. Pause as escritas da API e dos workers.
2. Restaure o ponto escolhido em um destino isolado.
3. Valide reservas conhecidas e a versão do esquema.
4. Reconcilie pagamentos do intervalo afetado.
5. Teste o caminho de criação antes de liberar tráfego.
6. Retome gradualmente e observe erros e filas.
```

Proteja os efeitos externos

Durante os testes, use provedores de sandbox e suspenda notificações reais. Compare registros do provedor com a base restaurada. Se reprocessar eventos, valide a origem e aplique deduplicação no intervalo recuperado. Preserve evidências antes de descartar a instância anterior.

Recuperação

Exercício resolvido

Cenário

O banco voltou ao estado das 09h55. O provedor confirma um pagamento às 09h58 para uma reserva que não aparece no banco restaurado. O mesmo evento pode ser entregue de novo.

Resolução

Recupere a referência ao pagamento pelo provedor e procure a reserva e a tentativa correspondentes. Se houver dados suficientes e o horário estiver livre, reconstrua a associação seguindo a regra do serviço. Caso haja conflito ou faltem dados, encaminhe para tratamento manual. Registre a operação recuperada com referência única ao pagamento para evitar duplicação.

Critério de aceite

Em homologação, use um pagamento fictício, processe o mesmo evento duas vezes e confira que existe uma única associação. Valide em seguida que a API voltou a listar e criar reservas.

Referências primárias

AWS Well-Architected — Teste de recuperação

Stripe — Webhooks e eventos duplicados

Recuperação

Verifique a retomada por etapas

Valide leitura e gravação antes de abrir o tráfego

Confira dados conhecidos, teste uma gravação fictícia e examine o estado do processamento em segundo plano. Defina sinais para interromper a retomada se as falhas voltarem.

Exercício adicional

A API responde à saúde, mas o worker ainda aponta para o banco antigo. O que fazer?

Resolução

Mantenha a retomada suspensa. Corrija o destino do worker e execute um caso de teste que confirme a gravação no banco restaurado e a atualização do histórico.

Ao assistir ao vídeo

Compare o ponto recuperável e o tempo até o serviço voltar.

Vídeo complementar

Disaster Recovery on AWS: Scenarios, RPO vs. RTO (em inglês)