IAM

Dê ao serviço só o acesso necessário

Pré-requisitos

Conheça papéis, buckets e chaves de objeto. O exercício usa Python 3.9 ou posterior e um bucket fictício. O serviço de geração grava comprovantes PDF. Outra parte da aplicação verifica autorização e atende downloads.

Separe confiança de permissões

A política de confiança de uma função define quem pode assumi-la. Uma política de permissões define ações e recursos acessíveis depois que a função é assumida. Use a identidade do ambiente de execução e as credenciais temporárias que ele fornece. O gerador e o serviço de leitura podem ter funções distintas.

Leia a política como principal, ação e recurso [1]

Na ausência de uma concessão aplicável, o pedido é negado. Uma negação explícita aplicável prevalece. A decisão efetiva pode depender também da política do bucket, limites de permissões e políticas da organização. Neste exercício, considere apenas a concessão de identidade apresentada.

Diferencie ARN de objeto e ARN de bucket [2]

PutObject opera sobre objetos e usa o ARN com barra e chave. ListBucket opera sobre o bucket e usa o ARN sem chave. Para escrita em um prefixo, restrinja o recurso a esse prefixo. Permissões adicionais de criptografia podem ser necessárias se o bucket usar uma chave AWS KMS gerenciada pelo cliente.

Mantenha no aplicativo as regras da agenda

A função é compartilhada pelo processo gerador. Ela restringe o que o processo pode fazer no S3. A aplicação ainda precisa conferir qual reserva pertence à unidade e qual chave pode ser gerada. Use identificadores internos e um bucket privado.

IAM

Exercício resolvido • Limite um gerador de PDFs

Enunciado

O gerador deve gravar R45 sob comprovantes/ no bucket fictício agenda-comprovantes-lab. Ele não precisa ler, listar ou apagar arquivos. Modele uma política de permissões para sua função e confira tentativas dentro e fora do prefixo.

1. Salve politica.json

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "GravarComprovantes",
    "Effect": "Allow",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::agenda-comprovantes-lab/comprovantes/*"
  }]
}
```

2. Salve verificar.py na mesma pasta

```
import json
from pathlib import Path

regra = json.loads(Path('politica.json').read_text(encoding='utf-8-sig'))
regra = regra['Statement'][0]
base = 'arn:aws:s3:::agenda-comprovantes-lab'
prefixo = regra['Resource'].removesuffix('*')

def permite(acao, recurso):
    return (regra['Effect'] == 'Allow' and acao == regra['Action']
            and recurso.startswith(prefixo))

arquivo = base + '/comprovantes/U12/R45/v1.pdf'
assert permite('s3:PutObject', arquivo)
assert not permite('s3:GetObject', arquivo)
assert not permite('s3:DeleteObject', arquivo)
assert not permite('s3:ListBucket', base)
assert not permite('s3:PutObject', base + '/exportacoes/R45.pdf')
print('Uma concessao e quatro recusas conferidas')
```

IAM

Valide a concessão e os limites do exercício

3. Execute python verificar.py

O script imprime 'Uma concessao e quatro recusas conferidas'. O modelo só avalia o efeito Allow, uma ação exata e um ARN com sufixo curinga. É uma verificação local do exercício. O IAM Policy Simulator tem regras e limites próprios [3].

Caso de erro • Abra toda a árvore de objetos

Troque /comprovantes/* por /* em Resource. A exportação passa a combinar com a regra, e o teste falha. Restaure o prefixo. Confira que a política concede somente a ação exigida pelo worker.

Variação • Um serviço separado lê PDFs

Modele para o leitor uma concessão s3:GetObject nos objetos do prefixo. O serviço autentica a pessoa e autoriza o acesso à reserva antes de ler. O gerador permanece com sua função de escrita. Se precisar verificar os bytes já existentes em uma recuperação, avalie a permissão de leitura como uma nova necessidade explícita.

Critérios para conferir

A escrita no prefixo corresponde à regra, assim como as quatro decisões negativas. Na conta de teste, valide a função efetivamente usada pela aplicação, o bucket e eventuais condições de criptografia. Confirme as operações permitidas e recusadas em um bucket sem dados de usuários.

Referências primárias

[1] AWS • Lógica de avaliação de políticas IAM

[2] AWS • Ações e tipos de recurso do Amazon S3

[3] AWS • Teste de políticas com IAM Policy Simulator

IAM

Isole leitura e gravação por responsabilidade

Modele a função de cada componente

O serviço que emite URLs de upload precisa das permissões associadas à operação assinada. Um worker que verifica anexos pode usar uma função distinta com leitura no prefixo esperado. Restrinja cada função ao ambiente correspondente.

Exercício adicional

O worker de verificação também consegue gravar anexos. Qual ajuste testar?

Resolução

Retire a concessão de gravação que não faz parte do trabalho. Use objetos de teste para verificar que o worker ainda lê anexos autorizados e que a função continua sem gravar ou apagar.

Ao assistir ao vídeo

Compare credenciais temporárias e permissões mínimas.

Vídeo complementar

Learn AWS IAM in less than 10 minutes (em inglês)