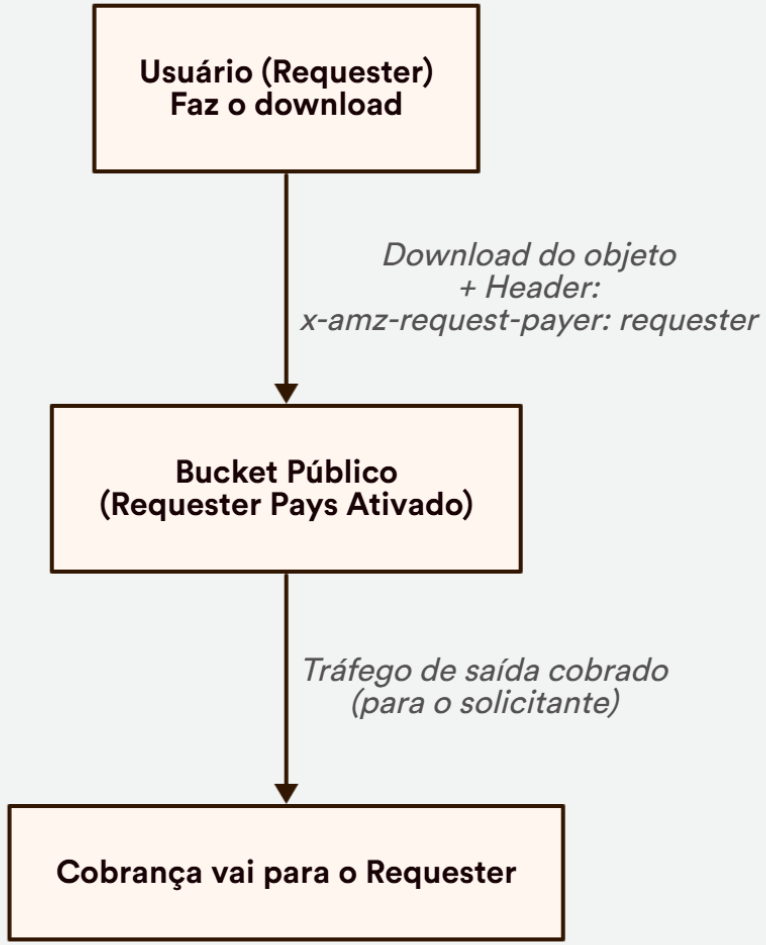
Amazon S3: Acesso Avançado – Requester Pays, Cross-Account, Logging

Requester Pays no S3

- Configuração onde quem faz o downloa paga pelo tráfego de saída
- Ideal para datasets públicos com alto volume de acesso
- Requer que o solicitante use `x-amz-request-payer: requester`
- Pode ser ativado por bucket via console ou API



Casos de Uso do Requester Pays

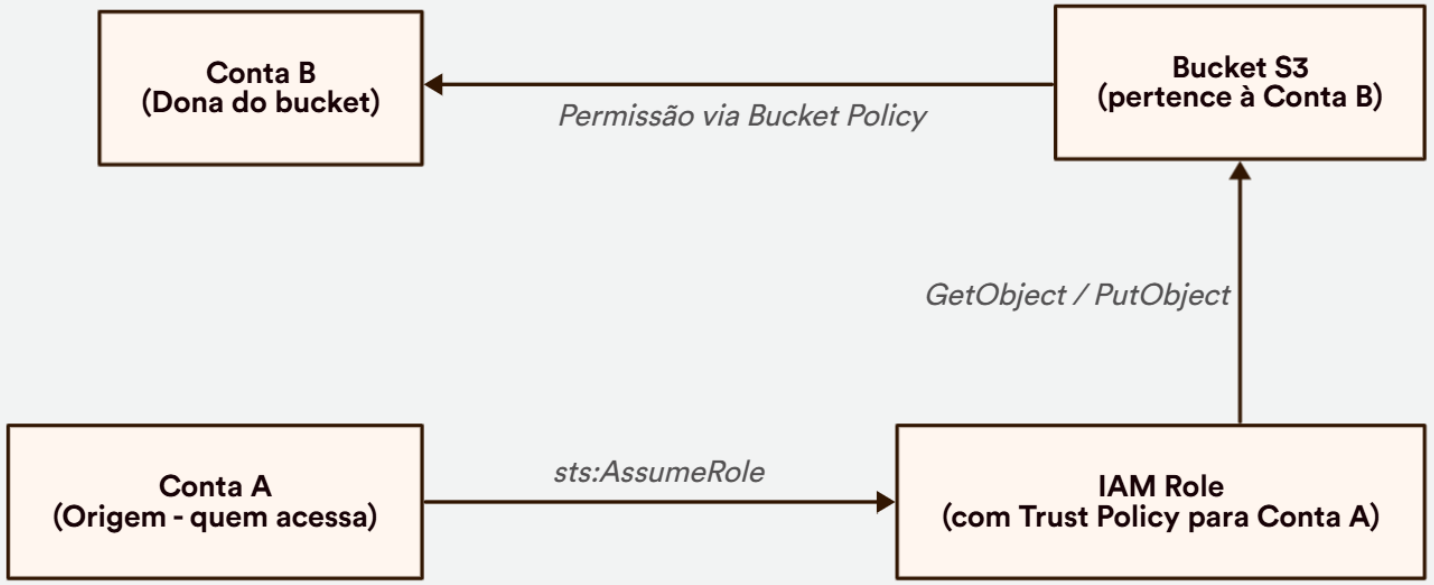
- Distribuição de datasets científicos ou governamentais
- Cenários onde múltiplos usuários externos acessam objetos grandes
- Evita que o dono do bucket assuma todos os custos de acesso

Acesso Cross-Account no S3

- Permite que contas diferentes acessem um mesmo bucket
- Pode ser feito com Bucket Policy, IAM Role com Trust Policy ou ambos
- Importante controlar ações específicas (ex: GetObject, PutObject)
- Boa prática: usar roles ao invés de permitir acesso direto

Exemplo: IAM Role Cross-Account

- Conta A define role com trust para Conta B
- Conta B assume a role via `sts:AssumeRole`
- Role tem permissões limitadas ao bucket desejado



1. Trust Policy – Permite Conta A assumir Role

```
{
  "Version": "2012-10-17",              ← Versão da política de permissões.
  "Statement": [                        ← Bloco de instruções.
    {
      "Effect": "Allow",                ← Permite que a ação definida abaixo seja executada.
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/NomeDaRole""  ← Conta A que poderá assumir essa role.
      },
      "Action": "sts:AssumeRole"        ← Ação que permite assumir a role via STS.
    }
  ]
}
```

2. Policy de Permissão – O que a role pode fazer

```
{
  "Version": "2012-10-17",              ← Versão da política de permissões.
  "Statement": [                        ← Bloco de instruções.
    {
      "Effect": "Allow",                ← Essa instrução permite as ações listadas.
      "Action": [                         ← Lista de ações que a role poderá executar.
        "s3:GetObject",               ← Permite leitura de objetos no bucket.
        "s3:PutObject"                ← Permite escrita de objetos no bucket.
      ],
      "Resource": "arn:aws:s3:::meu-bucket-compartilhado/*" ← Aponta para todos os objetos do bucket.
    }
  ]
}
```

Server Access Logging x CloudTrail

- S3 Server Access Logging: logs detalhados de acesso a objetos
- CloudTrail: logs de chamadas à API, incluindo ações administrativas
- Usar ambos fornece rastreabilidade completa e complementar
- Logs podem ser salvos em buckets dedicados

Boas Práticas e Dicas de Prova

- Use Requester Pays para distribuir datasets públicos pesados
- Prefira roles para acesso entre contas, com políticas restritivas
- CloudTrail ≠ Server Access Logging – são complementares
- Auditoria efetiva requer ativação de logs nos buckets corretos