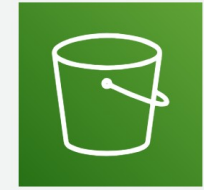


Amazon S3: Segurança, Logs, Encryption e Replicação

Segurança no Amazon S3



- Controle de acesso baseado em identidade (IAM Policies)
- Políticas baseadas em bucket (Bucket Policies)
- ACLs (Access Control Lists) — legado, uso limitado
- Integração com AWS Organizations e SCPs
- Recurso: Bloqueio de acesso público (Block Public Access)

Um passinho pra trás Voltando ao passado para entender antes as "ACLs"

CARACTERÍSTICA	ACL (ACCESS CONTROL LIST)	POLÍTICA DE BUCKET
Nível de controle	Objeto e bucket	Bucket (e objetos com condições)
Granularidade	Permissões simples (READ, WRITE)	Mais detalhada (ações, recursos, condições)
Flexibilidade	Limitada	Alta – pode restringir por IP, prefixo, etc.
Recomendação atual	<i>Legado – evitar quando possível</i>	✅ Recomendado
Permite acesso público?	Sim (via AllUsers ou AuthenticatedUsers)	Sim (via política com "Principal": "*")
Afetado pelo Block Public Access?	Sim	Sim
Dica para a prova	⚠ Usado historicamente, ainda pode aparecer em buckets antigos	🔒 Política de bucket + BPA ativo = combinação mais segura

Bloqueio de Acesso Público (Block Public Access)



- Configuração a nível de bucket e de conta
- Previne exposição acidental de dados sensíveis
- Boa prática de segurança padrão

CONFIGURAÇÃO	DESCRIÇÃO	DICA PARA A PROVA
Bloquear ACLs públicas novas	Impede que novas ACLs deem acesso público ao bucket ou objetos	🔒 ACLs são legadas. Use políticas modernas + bloqueio de ACLs
Bloquear ACLs públicas existentes	Remove ou ignora permissões públicas já atribuídas via ACLs	🚫 Impede acesso mesmo que ACL anterior permitisse
Bloquear políticas públicas	Evita que políticas de bucket permitam acesso público	⚠️ Mesmo que o JSON da policy permita, o acesso será negado
Aplicar restrições a todo bucket	Força o bloqueio global em todas as configurações públicas	✅ Boa prática padrão. Reforça segurança por padrão em novas contas

Política de Bucket S3 – Permitir Leitura Pública (s3:GetObject)

```
{
  "Version": "2012-10-17",           ← Versão da política (fixa).
  "Statement": [                     ← Lista de instruções (statements).
    {
      "Sid": "PublicReadGetObject",   ← Identificador opcional da regra.
      "Effect": "Allow",              ← Permitir o acesso descrito abaixo.
      "Principal": "*",               ← Qualquer entidade (acesso público).
      "Action": "s3:GetObject",        ← Permite ler objetos (download).
      "Resource": "arn:aws:s3:::meu-bucket/*" ← Aponta para todos os objetos do bucket.
    }
  ]
}
```

Política com Condição – Acesso somente de IP específico

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGetFromSpecificIP",
      "Effect": "Allow",
      "Principal": "*",               ← Qualquer usuário, mas com condição.
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::meu-bucket-restrito/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "200.100.50.0/24" ← Apenas IPs dessa faixa podem acessar.
        }
      }
    }
  ]
}
```



Logs de Acesso no S3

- S3 Server Access Logging: registra requisições feitas ao bucket
- Pode ser direcionado para outro bucket
- Usado para auditoria, debugging, e análise de acesso





AWS CloudTrail com S3





- CloudTrail registra chamadas à API (ex: PUT, DELETE)
- Permite rastrear alterações, uploads e exclusões
- Integração recomendada para auditoria completa





Criptografia no S3 (Encryption)

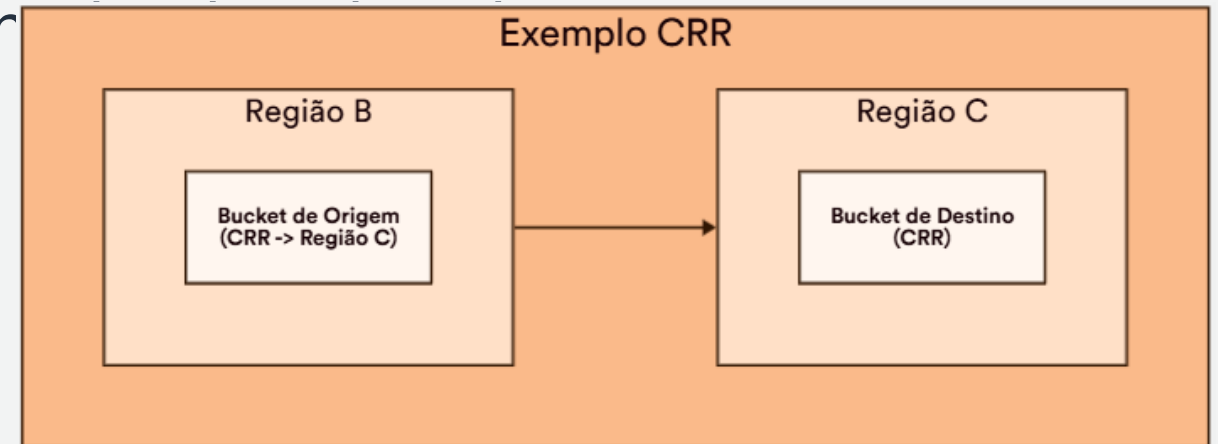
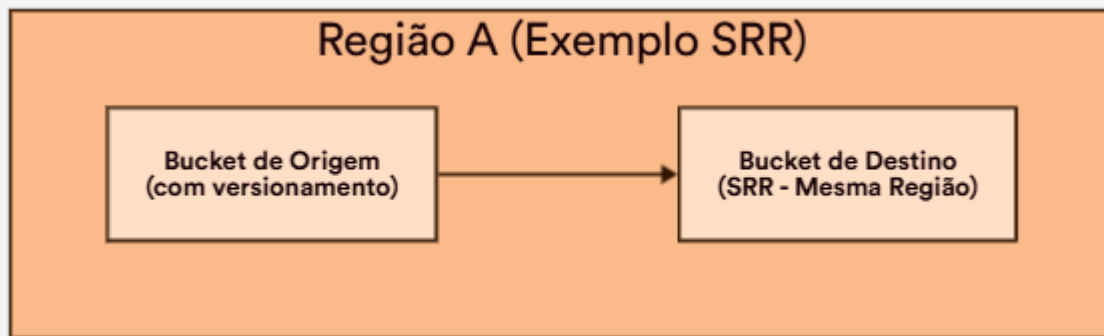
- Criptografia em repouso: SSE-S3, SSE-KMS, SSE-C
- SSE-S3: AWS gerencia as chaves
- SSE-KMS: chaves no AWS Key Management Service (KMS)
- SSE-C: cliente fornece as chaves (menos usado)

TIPO	GERENCIAMENTO DE CHAVES	USO	DICA PARA A PROVA
SSE-S3	AWS gerencia tudo automaticamente	Padrão, sem configuração adicional	 Mais simples. Aparece como “SSE” nas provas (sem sufixo!)
SSE-KMS	Gerenciada pelo AWS KMS (suporte a CMKs e logs)	Mais controle e auditoria, pode usar chave própria	 Pode gerar custo por requisição. Exige permissão adicional (kms:Encrypt)
SSE-C	Cliente envia a chave a cada operação	Uso raro. AWS não armazena a chave	 Não é compatível com SDKs ou integração com KMS. Muito incomum na prática
HTTPS (trânsito)	Obrigatório por padrão	Protege dados em movimento	 A prova pode perguntar sobre isso como “criptografia em trânsito”



Replicação entre Regiões (CRR) e Mesma Região (SRR)

- Cross-Region Replication (CRR): cópia automática para outra região
- Same-Region Replication (SRR): replicação dentro da mesma região
- Útil para backup, conformidade e menor latência de leitura
- Requer versionamento ativado



Boas Práticas e Dicas de Prova

- Sempre habilite Block Public Access, exceto em casos controlados
- Use políticas ao invés de ACLs para controle de acesso
- Combine logs do S3 + CloudTrail para auditoria robusta
- Prefira SSE-KMS para maior controle sobre chaves
- Versionamento é pré-requisito para replicação