



GUIA DO CLIENTE · OBJECT STORAGE S3

AWS CLI com Object Storage S3

Instalação, configuração e uso do AWS CLI
para gerenciar seus buckets e arquivos

Ficha do documento

VERSÃO	1.0
DATA	23/10/2026
ENDPOINT	https://s3.altatech.cloud
FERRAMENTA	AWS CLI v2 (≥ 2.13 · recomendado ≥ 2.23)
PÚBLICO	Clientes do serviço Object Storage S3
SUPORTE	Equipe de suporte Altatech

Sumário

Clique em um item para ir à seção. O painel de marcadores do leitor de PDF mostra a mesma estrutura.

1. Visão geral	4
1.1 Como funciona	4
1.2 Dados de acesso fornecidos pela Altatech	4
1.3 Conceitos	5
1.4 Convenções deste guia	5
2. Instalação do AWS CLI v2	6
2.1 Requisitos	6
2.2 Linux (x86_64 e ARM64)	6
2.3 macOS (Intel e Apple Silicon)	6
2.4 Windows	7
2.5 Verificação, atualização e autocompletar	7
3. Configuração do perfil e alias	8
3.1 Arquivos de configuração	8
3.2 Criar o perfil (modo interativo)	8
3.3 Arquivos finais (referência)	8
3.4 Parâmetros explicados	9
3.5 Alias de shell	9
3.6 Variáveis de ambiente (scripts e automação)	10
3.7 Testar a conexão	10
3.8 Ordem de precedência	10
4. Buckets	12
4.1 Comandos s3 × s3api	12
4.2 Regras de nomenclatura	12
4.3 Criar bucket	12
4.4 Listar e inspecionar	13
4.5 Remover bucket	13
5. Arquivos (objetos)	14
5.1 Enviar e baixar	14
5.2 Sincronizar diretórios	14
5.3 Copiar, mover e renomear	14

5.4 Excluir	15
5.5 Metadados e tipo de conteúdo	15
5.6 Compartilhar com link temporário	15
6. Versionamento e recuperação	16
6.1 Habilitar e consultar	16
6.2 Listar versões de um arquivo	16
6.3 Recuperar uma versão anterior	16
6.4 Desfazer uma exclusão	16
6.5 Excluir versões definitivamente	17
7. Object Lock (imutabilidade)	18
7.1 Para que serve	18
7.2 Requisitos	18
7.3 Criar um bucket com Object Lock	19
7.4 Modos de retenção	19
7.5 Retenção padrão do bucket	20
7.6 Retenção por objeto	20
7.7 Legal hold	20
7.8 Consultar a proteção de um objeto	21
7.9 Comportamento em exclusões e sobrescritas	21
8. Criptografia (SSE-S3)	22
8.1 O que é e para que serve	22
8.2 Modalidades disponíveis	22
8.3 Ativar a criptografia padrão no bucket	22
8.4 Solicitar a criptografia em um envio	23
8.5 Verificar se um objeto está criptografado	23
8.6 Pontos de atenção	24
9. Boas práticas	25
9.1 Exemplo: backup diário agendado (Linux)	25
10. Solução de problemas	26
10.1 Diagnóstico detalhado	27
11. Referência rápida	28

1 Visão geral

O que você precisa antes de começar

Este guia mostra como instalar e configurar o **AWS CLI v2** para acessar o serviço de **Object Storage S3 da Altatech** e como gerenciar seus buckets e arquivos pela linha de comando. O serviço é compatível com a API S3, então os mesmos comandos usados com a AWS funcionam aqui, bastando apontar o CLI para o endpoint da Altatech.

1.1 Como funciona



Figura 1 — Caminho de uma requisição do AWS CLI até os seus dados

O AWS CLI lê o perfil configurado no seu computador, assina cada requisição com a sua access key e secret key e a envia via HTTPS ao endpoint da Altatech. O serviço valida a credencial e executa a operação nos buckets aos quais você tem acesso.

1.2 Dados de acesso fornecidos pela Altatech

Dado	Exemplo neste guia	Para que serve
Endpoint	<code>https://s3.altatech.cloud</code>	Endereço do serviço. Substitui os endereços da AWS.
Access Key ID	<code>EXAMPLEKEY0000000001</code>	Identificador da sua credencial (equivalente a um usuário).
Secret Access Key	(40 caracteres)	Segredo usado para assinar as requisições (equivalente a uma senha).
Região	<code>south-br-1</code>	Valor fixo, sempre o mesmo. Usado na assinatura das requisições.

Com essas credenciais você tem acesso completo ao seu armazenamento: pode criar, listar e remover buckets e arquivos sem depender de ninguém. Os buckets são criados por você mesmo (seção 4).

IMPORTANTE Esta credencial dá **acesso total** a todo o seu armazenamento. Trate a Secret Access Key como uma senha: não a envie por e-mail ou chat, não a coloque em repositórios de código e não a compartilhe entre pessoas. Em caso de suspeita de vazamento, solicite imediatamente uma nova credencial ao suporte da Altatech.

1.3 Conceitos

Termo	Significado
Bucket	Contêiner de armazenamento. Funciona como uma pasta raiz com nome único.
Objeto	Cada arquivo armazenado no bucket.
Chave (key)	Nome completo do objeto dentro do bucket, ex.: <code>2026/10/relatorio.pdf</code> .
Prefixo	Parte inicial da chave, usada como "pasta", ex.: <code>2026/10/</code> .
URI S3	Forma de referenciar bucket e objeto nos comandos: <code>s3://bucket/chave</code> .
Perfil	Conjunto nomeado de configurações do AWS CLI (endpoint, região, credencial).

1.4 Convenções deste guia

Valor usado no guia	Significado
<code>https://s3.altatech.cloud</code>	Endpoint do serviço
<code>altatech</code>	Nome do perfil do AWS CLI
<code>s3alt</code>	Atalho (alias) para <code>aws --profile altatech</code>
<code>empresa-backup</code>	Bucket de exemplo; crie o seu na seção 4

Os blocos de código têm um rótulo no topo (**BASH**, **POWERSHELL**, **INI**, **SAÍDA**). Linhas em azul-claro são comentários. Os avisos seguem quatro níveis:

NOTA Informação complementar.

DICA Atalho ou forma mais eficiente de fazer a mesma coisa.

ATENÇÃO Ponto em que é comum errar; leia antes de executar.

IMPORTANTE Ação com impacto de segurança ou irreversível.

2 Instalação do AWS CLI v2

Instalador oficial em Linux, macOS e Windows

2.1 Requisitos

Item	Requisito	Motivo
Versão mínima	2.13 ou superior	Permite gravar o endpoint dentro do perfil.
Versão recomendada	2.23 ou superior	Suporte às opções de checksum usadas na configuração.
Linux	<code>unzip</code> , <code>curl</code>	Download e extração do instalador oficial.
Acesso	<code>sudo</code> / administrador	Instalação no sistema.

ATENÇÃO Evite `apt install awscli` / `pip install awscli`. Esses pacotes costumam entregar a versão 1 ou uma versão 2 desatualizada. Use sempre o instalador oficial abaixo.

2.2 Linux (x86_64 e ARM64)

BASH

```
# 1. Baixar o instalador (x86_64)
curl -fsSL "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o awscliv2.zip

# 1. (alternativa) servidores ARM64 / aarch64
curl -fsSL "https://awscli.amazonaws.com/awscli-exe-linux-aarch64.zip" -o awscliv2.zip

# 2. Extrair e instalar
unzip -q awscliv2.zip
sudo ./aws/install

# 3. Conferir
aws --version
```

2.3 macOS (Intel e Apple Silicon)

› Opção A — pacote oficial (.pkg universal)

BASH

```
curl -fsSL "https://awscli.amazonaws.com/AWSCLIV2.pkg" -o AWSCLIV2.pkg
sudo installer -pkg AWSCLIV2.pkg -target /
aws --version
```

› Opção B — Homebrew

BASH

```
brew install awscli
aws --version
```

2.4 Windows

POWERSHELL

```
# PowerShell como administrador
msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi

# Abra um NOVO terminal e confira
aws --version
```

2.5 Verificação, atualização e autocompletar

A saída de `aws --version` deve começar com `aws-cli/2.`. Exemplo:

SAÍDA

```
aws-cli/2.31.x Python/3.13.x Linux/6.x exe/x86_64
```

› Atualizar uma instalação existente (Linux)

BASH

```
curl -fsSL "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o awscliv2.zip
unzip -qo awscliv2.zip
sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --update
```

› Autocompletar com TAB

BASH

```
# bash (adicione ao ~/.bashrc)
complete -C '/usr/local/bin/aws_completer' aws

# zsh (adicione ao ~/.zshrc)
autoload bashcompinit && bashcompinit
autoload -Uz compinit && compinit
complete -C '/usr/local/bin/aws_completer' aws
```

DICA No macOS com Homebrew, o caminho costuma ser `/opt/homebrew/bin/aws_completer`. Confira com `which aws_completer`.

3 Configuração do perfil e alias

Endpoint, access key e secret key configurados uma única vez

Um **perfil** guarda endpoint, região e credencial com um nome. Depois de criado, nenhum comando precisa repetir `--endpoint-url` ou as chaves. O **alias de shell** encurta ainda mais a digitação.

3.1 Arquivos de configuração

Arquivo	Conteúdo	Cabeçalho da seção
<code>~/.aws/credentials</code>	Somente segredos: access key e secret key	<code>[altatech]</code>
<code>~/.aws/config</code>	Endpoint, região, formato de saída, opções de S3	<code>[profile altatech]</code>

ATENÇÃO No `config` o cabeçalho leva o prefixo `profile` (`[profile altatech]`); no `credentials`, não (`[altatech]`). No Windows os arquivos ficam em `%USERPROFILE%\ .aws\`.

3.2 Criar o perfil (modo interativo)

```
BASH

aws configure --profile altatech
# AWS Access Key ID [None]: <SUA_ACCESS_KEY>
# AWS Secret Access Key [None]: <SUA_SECRET_KEY>
# Default region name [None]: south-br-1
# Default output format [None]: json

# Endpoint e opções de compatibilidade
aws configure set endpoint_url https://s3.altatech.cloud --profile altatech
aws configure set request_checksum_calculation when_required --profile altatech
aws configure set response_checksum_validation when_required --profile altatech
```

Depois, abra `~/.aws/config` e acrescente o bloco `s3`, deixando o arquivo como na seção 3.3.

3.3 Arquivos finais (referência)

```
INI · ~/.aws/credentials

[altatech]
aws_access_key_id      = EXAMPLEKEY000000000001
aws_secret_access_key  = exemploSecretKey00000000000000000000000000000000
```

```
INI · ~/.aws/config

[profile altatech]
region                = south-br-1
output                = json
endpoint_url          = https://s3.altatech.cloud
request_checksum_calculation = when_required
response_checksum_validation = when_required
s3 =
    addressing_style = path
```

BASH

```
# Proteja os arquivos: somente o seu usuário pode ler
chmod 700 ~/.aws
chmod 600 ~/.aws/credentials ~/.aws/config
```

3.4 Parâmetros explicados

Parâmetro	Valor	Por que configurar
endpoint_url	https://s3.altatech.cloud	Direciona os comandos ao serviço da Altatech em vez da AWS.
region	south-br-1	Valor fixo do serviço, usado na assinatura das requisições. Mantenha exatamente este valor.
addressing_style	path	Gera URLs no formato <code>https://endpoint/bucket/objeto</code> , compatível com o serviço.
request_checksum_calculation	when_required	Garante compatibilidade de uploads com o serviço (necessário no CLI ≥ 2.23).
response_checksum_validation	when_required	Mesma razão, nos downloads.
output	json	Formato de saída. Alternativas: <code>table</code> , <code>text</code> , <code>yaml</code> .

▸ Ajuste opcional para arquivos grandes

Para backups e arquivos de vários GB, os parâmetros abaixo controlam o envio em partes (multipart). Acrescente-os dentro do bloco `s3 =` do `~/.aws/config`:

INI · ~/.aws/config

```
s3 =
  addressing_style      = path
  multipart_threshold   = 64MB
  multipart_chunksize   = 64MB
  max_concurrent_requests = 10
```

3.5 Alias de shell

O alias evita digitar `--profile altatech` em todo comando.

BASH

```
# Adicione ao ~/.bashrc (Linux) ou ~/.zshrc (macOS)
alias s3alt='aws --profile altatech'

# Recarregue o shell
source ~/.zshrc      # ou: source ~/.bashrc

# Uso
s3alt s3 ls
```

POWERSHELL

```
# Windows: adicione ao arquivo indicado por $PROFILE
function s3alt { aws --profile altatech @args }
```

ATENÇÃO Aliases só funcionam no shell interativo. Dentro de scripts `.sh`, use `aws --profile altatech` ou `export AWS_PROFILE=altatech` no início do script.

DICA Se a versão do CLI for anterior à 2.13, inclua o endpoint no próprio alias: `alias s3alt='aws --profile altatech --endpoint-url https://s3.altatech.cloud'`.

3.6 Variáveis de ambiente (scripts e automação)

Em scripts, agendamentos ou containers, as variáveis de ambiente substituem os arquivos de perfil:

BASH

```
export AWS_ACCESS_KEY_ID="EXAMPLEKEY0000000001"
export AWS_SECRET_ACCESS_KEY="exemploSecretKey00000000000000000000000000000000"
export AWS_ENDPOINT_URL="https://s3.altatech.cloud"
export AWS_DEFAULT_REGION="south-br-1"
export AWS_REQUEST_CHECKSUM_CALCULATION="when_required"
export AWS_RESPONSE_CHECKSUM_VALIDATION="when_required"

# Ou apenas selecione um perfil existente para a sessão inteira
export AWS_PROFILE=altatech
```

3.7 Testar a conexão

BASH

```
aws configure list-profiles      # perfis existentes
aws configure list --profile altatech # valores efetivos (chaves mascaradas) e origem
s3alt s3 ls                     # lista os seus buckets
```

NOTA Se esta for a primeira vez que você acessa, a listagem vem **vazia**: isso indica que a conexão e as credenciais estão corretas. O próximo passo é criar o seu primeiro bucket (seção 4.3).

3.8 Ordem de precedência

Quando o mesmo parâmetro é definido em mais de um lugar, vence o de maior prioridade:

Prioridade	Origem	Exemplo
1 (maior)	Opção na linha de comando	<code>--endpoint-url</code> , <code>--profile</code> , <code>--region</code>
2	Variáveis de ambiente	<code>AWS_ENDPOINT_URL</code> , <code>AWS_ACCESS_KEY_ID</code> , <code>AWS_PROFILE</code>
3	Arquivos do perfil	<code>~/.aws/credentials</code> , <code>~/.aws/config</code>

ATENÇÃO Variáveis `AWS_ACCESS_KEY_ID` / `AWS_SECRET_ACCESS_KEY` esquecidas no terminal têm prioridade sobre o perfil e podem causar `AccessDenied` ou `InvalidAccessKeyId`. Confira com `aws configure list` (a coluna **Type** mostra `env`).

4 Buckets

Criação, listagem, inspeção e remoção

4.1 Comandos s3 × s3api

Família	Nível	Use para
aws s3	Alto nível, estilo <code>cp</code> / <code>ls</code> / <code>sync</code>	Operações do dia a dia com arquivos e diretórios.
aws s3api	Baixo nível, 1 comando = 1 operação da API	Configurações finas: versionamento, metadados, versões.

4.2 Regras de nomenclatura

Regra	Válido	Inválido
De 3 a 63 caracteres	<code>empresa-backup</code>	<code>ab</code>
Somente minúsculas, números, hífen e ponto	<code>empresa-logs-2026</code>	<code>Empresa_Logs</code>
Começar e terminar com letra ou número	<code>dados-app01</code>	<code>-dados-</code>
Não ter formato de endereço IP	<code>backup-10-0-0-1</code>	<code>10.0.0.1</code>
Evitar pontos no nome	<code>site-empresa</code>	<code>site.empresa</code>
Único no serviço	—	nome em uso → <code>BucketAlreadyExists</code>

4.3 Criar bucket

Como você tem acesso completo, pode criar quantos buckets precisar. Uma boa prática é usar um bucket por finalidade (ex.: `empresa-backup`, `empresa-logs`, `empresa-site`).

NOTA Para criar um bucket **imutável** (Object Lock), o procedimento é diferente: o bucket precisa ser criado já com o placement target `immutable-placement`. Veja a seção 7.

BASH

```
# Forma simples
s3alt s3 mb s3://empresa-backup

# Forma equivalente via API
s3alt s3api create-bucket --bucket empresa-backup
```

4.4 Listar e inspecionar

BASH

```
s3alt s3 ls                                # buckets visíveis para a credencial
s3alt s3api head-bucket --bucket empresa-backup # sem saída = existe e há acesso
s3alt s3 ls s3://empresa-backup           # primeiro nível do bucket
s3alt s3 ls s3://empresa-backup/2026/     # conteúdo de um prefixo ("pasta")
```

› Espaço utilizado

BASH

```
s3alt s3 ls s3://empresa-backup --recursive --human-readable --summarize
```

SAÍDA · últimas linhas

```
...
Total Objects: 1284
Total Size: 412.7 GiB
```

4.5 Remover bucket

BASH

```
s3alt s3 rb s3://empresa-backup           # só funciona se estiver vazio
s3alt s3 rb s3://empresa-backup --force   # apaga todos os objetos e depois o bucket
```

IMPORTANTE A remoção é **irreversível**: os dados não podem ser recuperados. Em bucket com versionamento habilitado, `--force` não remove as versões antigas e o comando falha com `BucketNotEmpty` ; veja a seção 6.5.

5 Arquivos (objetos)

Enviar, baixar, sincronizar, mover, excluir e compartilhar

5.1 Enviar e baixar

BASH

```
# Enviar um arquivo
s3alt s3 cp ./dump.sql.gz s3://empresa-backup/2026/10/dump.sql.gz

# Baixar um arquivo
s3alt s3 cp s3://empresa-backup/2026/10/dump.sql.gz ./restaurado.sql.gz

# Enviar / baixar um diretório inteiro
s3alt s3 cp ./relatorios s3://empresa-backup/relatorios/ --recursive
s3alt s3 cp s3://empresa-backup/relatorios/ ./relatorios --recursive

# Filtrar por padrão de nome
s3alt s3 cp ./logs s3://empresa-backup/logs/ --recursive --exclude "*" --include "*.gz"
```

NOTA O CLI divide automaticamente arquivos grandes em partes e envia em paralelo. Para ajustar esse comportamento, veja "Ajuste opcional para arquivos grandes" na seção 3.4.

5.2 Sincronizar diretórios

BASH

```
# Envia apenas arquivos novos ou alterados
s3alt s3 sync ./relatorios s3://empresa-backup/relatorios/

# Baixa apenas o que mudou no bucket
s3alt s3 sync s3://empresa-backup/relatorios/ ./relatorios

# Espelhar: remove no destino o que não existe mais na origem
s3alt s3 sync ./relatorios s3://empresa-backup/relatorios/ --delete
```

DICA Antes de qualquer `sync --delete`, `mv` ou `rm --recursive`, rode o mesmo comando com `--dryrun`: ele mostra o que seria feito sem alterar nada.

5.3 Copiar, mover e renomear

BASH

```
# Copiar dentro do serviço (sem baixar para a sua máquina)
s3alt s3 cp s3://empresa-backup/a.pdf s3://empresa-backup/arquivo/a.pdf

# Mover / renomear
s3alt s3 mv s3://empresa-backup/a.pdf s3://empresa-backup/a-2026.pdf

# Mover um prefixo inteiro
s3alt s3 mv s3://empresa-backup/temp/ s3://empresa-backup/processado/ --recursive
```

5.4 Excluir

BASH

```
s3alt s3 rm s3://empresa-backup/2026/10/dump.sql.gz      # um objeto
s3alt s3 rm s3://empresa-backup/temp/ --recursive      # todo um prefixo
s3alt s3 rm s3://empresa-backup/temp/ --recursive --dryrun # simular antes
```

IMPORTANTE Sem versionamento habilitado, objetos excluídos ou sobrescritos **não podem ser recuperados**. Para dados críticos, habilite o versionamento (seção 6).

5.5 Metadados e tipo de conteúdo

BASH

```
# Detalhes de um objeto (tamanho, data, ETag, tipo, metadados)
s3alt s3api head-object --bucket empresa-backup --key 2026/10/dump.sql.gz

# Definir o tipo de conteúdo e metadados no envio
s3alt s3 cp ./index.html s3://empresa-backup/site/index.html \
  --content-type "text/html" --metadata origem=erp,versao=3
```

5.6 Compartilhar com link temporário

O comando `presign` gera uma URL assinada que permite **baixar** o objeto sem credencial, por tempo limitado. Útil para enviar um arquivo a um terceiro sem dar acesso ao bucket.

BASH

```
# Link válido por 1 hora (3600 s). Máximo: 7 dias (604800 s)
s3alt s3 presign s3://empresa-backup/2026/10/relatorio.pdf --expires-in 3600
```

SAÍDA

```
https://s3.altatech.cloud/empresa-backup/2026/10/relatorio.pdf?X-Amz-Algorithm=...
```

ATENÇÃO Qualquer pessoa com o link consegue baixar o arquivo até a expiração. Use o menor prazo possível e não publique esses links.

6 Versionamento e recuperação

Proteção contra exclusões e sobrescritas acidentais

Com o versionamento habilitado, cada sobrescrita gera uma nova versão do objeto e cada exclusão apenas cria um **marcador de exclusão** (delete marker). As versões anteriores continuam disponíveis para recuperação.

6.1 Habilitar e consultar

BASH

```
s3alt s3api put-bucket-versioning --bucket empresa-backup \
    --versioning-configuration Status=Enabled

s3alt s3api get-bucket-versioning --bucket empresa-backup
```

NOTA Uma vez habilitado, o versionamento só pode ser **suspenso** (`Status=Suspended`), não desabilitado. Versões antigas ocupam espaço e contam no seu armazenamento até serem excluídas.

6.2 Listar versões de um arquivo

BASH

```
s3alt s3api list-object-versions --bucket empresa-backup --prefix relatorios/vendas.xlsx \
    --query "Versions[][VersionId,LastModified,Size,IsLatest]" --output table
```

6.3 Recuperar uma versão anterior

BASH

```
# Baixar uma versão específica
s3alt s3api get-object --bucket empresa-backup --key relatorios/vendas.xlsx \
    --version-id <VERSION_ID> ./vendas-versao-anterior.xlsx

# Tornar essa versão a atual novamente (copia sobre a atual)
s3alt s3api copy-object --bucket empresa-backup --key relatorios/vendas.xlsx \
    --copy-source "empresa-backup/relatorios/vendas.xlsx?versionId=<VERSION_ID>"
```

6.4 Desfazer uma exclusão

Ao excluir um objeto versionado, ele some da listagem, mas as versões continuam guardadas. Para restaurá-lo, remova o marcador de exclusão:

BASH

```
# 1. Localizar o marcador de exclusão
s3alt s3api list-object-versions --bucket empresa-backup --prefix relatorios/vendas.xlsx \
    --query "DeleteMarkers[][VersionId,LastModified,IsLatest]" --output table

# 2. Remover o marcador (o objeto volta a aparecer)
s3alt s3api delete-object --bucket empresa-backup --key relatorios/vendas.xlsx \
    --version-id <VERSION_ID_DO_MARCADOR>
```

6.5 Excluir versões definitivamente

BASH

```
# Remove permanentemente UMA versão (irreversível)
s3alt s3api delete-object --bucket empresa-backup --key relatorios/vendas.xlsx \
  --version-id <VERSION_ID>
```

IMPORTANTE Excluir informando `--version-id` apaga aquela versão **definitivamente**. Para esvaziar um bucket versionado antes de removê-lo, todas as versões e marcadores precisam ser excluídos dessa forma.

7 Object Lock (imutabilidade)

Proteção WORM contra exclusão e alteração de objetos

O **Object Lock** impede que versões de objetos sejam **excluídas ou sobrescritas** durante um período definido, ou por tempo indeterminado. É o modelo **WORM** ("write once, read many"): o dado é gravado uma vez e pode ser lido quantas vezes for preciso, mas não pode ser apagado nem alterado enquanto estiver protegido.

7.1 Para que serve

- **Backups protegidos** contra ransomware, exclusão acidental e credenciais comprometidas.
- **Retenção obrigatória** de contratos, documentos fiscais e logs de auditoria.
- **Preservação de evidências** enquanto houver litígio ou investigação (legal hold).

Conceito	Descrição
Retenção (retention)	Período em que a versão do objeto fica protegida, definido por uma data final. Depois dela, a proteção expira.
Legal hold	Proteção sem data de expiração . Permanece até ser removida explicitamente.
Modo de retenção	<code>GOVERNANCE</code> ou <code>COMPLIANCE</code> : define o quão rígida é a retenção (seção 7.4).
Versão do objeto	O lock protege cada versão do objeto. Por isso o versionamento é obrigatório (seção 6).

7.2 Requisitos

Requisito	Detalhe
Habilitado na criação	O Object Lock só pode ser ativado ao criar o bucket (<code>--object-lock-enabled-for-bucket</code>). Buckets existentes não podem ser convertidos.
Placement target	O bucket deve ser criado no placement target <code>immutable-placement</code> . O placement target define em qual área de armazenamento do serviço o bucket é criado e não pode ser alterado depois .
Versionamento	Habilitado automaticamente na criação do bucket e não pode ser suspenso .
Comando	Use <code>s3api create-bucket</code> . O atalho <code>s3 mb</code> não aceita essas opções.

IMPORTANTE Todo bucket com Object Lock deve ser criado com o placement target `immutable-placement`. Como o Object Lock e o placement target não podem ser alterados depois da criação, um bucket criado sem eles precisa ser **recriado**: crie um novo bucket da forma correta e migre os dados com `s3 sync`.

7.3 Criar um bucket com Object Lock

BASH

```
s3alt s3api create-bucket --bucket empresa-imutavel \
  --object-lock-enabled-for-bucket \
  --create-bucket-configuration LocationConstraint=south-br-1:immutable-placement
```

Parte do comando	Função
--object-lock-enabled-for-bucket	Cria o bucket com Object Lock (e com o versionamento habilitado).
LocationConstraint=south-br-1:immutable-placement	Formato <code>região:placement</code> . A região é sempre <code>south-br-1</code> ; depois dos dois-pontos vem o placement target <code>immutable-placement</code> .

Confirme que o bucket foi criado com o Object Lock ativo:

BASH

```
s3alt s3api get-object-lock-configuration --bucket empresa-imutavel
```

JSON · saída

```
{
  "ObjectLockConfiguration": {
    "ObjectLockEnabled": "Enabled"
  }
}
```

DICA Escreva o `LocationConstraint` exatamente como no exemplo, sem espaços: `south-br-1:immutable-placement`. Se o serviço responder `InvalidLocationConstraint`, revise a região e o nome do placement target.

7.4 Modos de retenção

Característica	GOVERNANCE	COMPLIANCE
Proteção	Protege contra exclusão e alteração por usuários comuns.	Proteção máxima e inflexível.
Pode ser contornado?	Sim, por quem tem permissão, usando <code>--bypass-governance-retention</code> .	Não. Nem mesmo com a credencial de acesso total.
Reduzir ou remover a retenção	Possível (com bypass).	Impossível. Só é permitido estender o prazo.
Uso indicado	Testes e proteção contra erros operacionais.	Backups imutáveis e retenção regulatória.

IMPORTANTE Uma retenção em modo **COMPLIANCE** não pode ser desfeita por ninguém até a data final. Antes de usá-lo em produção, valide o procedimento em um bucket de teste com modo **GOVERNANCE** e prazo curto (por exemplo, 1 dia).

7.5 Retenção padrão do bucket

A retenção padrão é aplicada automaticamente a **todas as novas versões** gravadas no bucket, inclusive as enviadas por `s3 cp` e `s3 sync`. Informe o prazo em `Days` ou em `Years`, nunca nos dois.

BASH

```
s3alt s3api put-object-lock-configuration --bucket empresa-imutavel \
--object-lock-configuration '{
  "ObjectLockEnabled": "Enabled",
  "Rule": { "DefaultRetention": { "Mode": "GOVERNANCE", "Days": 30 } }
}'
```

NOTA A retenção padrão vale apenas para versões gravadas **depois** da configuração. Versões que já existiam no bucket não são alteradas.

DICA No PowerShell/Windows, grave o JSON em um arquivo (`lock.json`) e use `--object-lock-configuration file://lock.json`, evitando problemas de aspas.

7.6 Retenção por objeto

Para definir um modo e uma data específicos, envie o objeto com `s3api put-object`:

BASH

```
s3alt s3api put-object --bucket empresa-imutavel --key contratos/c-001.pdf \
--body ./c-001.pdf \
--object-lock-mode COMPLIANCE \
--object-lock-retain-until-date 2027-12-31T00:00:00Z
```

Para aplicar ou **estender** a retenção de uma versão que já existe:

BASH

```
s3alt s3api put-object-retention --bucket empresa-imutavel --key contratos/c-001.pdf \
--version-id <VERSION_ID> \
--retention Mode=COMPLIANCE,RetainUntilDate=2028-12-31T00:00:00Z
```

NOTA As opções de lock existem no `s3api put-object`; os comandos `aws s3 cp` e `aws s3 sync` não as aceitam. Para envios em massa, use a retenção padrão (seção 7.5).

7.7 Legal hold

O legal hold protege a versão sem prazo e **independe da retenção**: enquanto qualquer um dos dois estiver ativo, a versão não pode ser excluída.

BASH

```
# Ativar
s3alt s3api put-object-legal-hold --bucket empresa-imutavel --key contratos/c-001.pdf \
--version-id <VERSION_ID> --legal-hold Status=ON

# Remover
s3alt s3api put-object-legal-hold --bucket empresa-imutavel --key contratos/c-001.pdf \
--version-id <VERSION_ID> --legal-hold Status=OFF
```

7.8 Consultar a proteção de um objeto

BASH

```
s3alt s3api head-object --bucket empresa-imutavel --key contratos/c-001.pdf
s3alt s3api get-object-retention --bucket empresa-imutavel --key contratos/c-001.pdf
s3alt s3api get-object-legal-hold --bucket empresa-imutavel --key contratos/c-001.pdf
```

JSON · saída (trecho do head-object)

```
{
  "ObjectLockMode": "COMPLIANCE",
  "ObjectLockRetainUntilDate": "2027-12-31T00:00:00+00:00",
  "ObjectLockLegalHoldStatus": "OFF"
}
```

7.9 Comportamento em exclusões e sobrescritas

Operação	Resultado em uma versão protegida
Excluir sem informar a versão (<code>s3 rm</code>)	Cria um marcador de exclusão : o objeto some da listagem, mas a versão protegida continua armazenada e pode ser recuperada (seção 6.4).
Excluir uma versão específica (<code>--version-id</code>)	Negado (<code>AccessDenied</code>) enquanto houver retenção ativa ou legal hold.
Sobrescrever (novo envio na mesma chave)	Cria uma nova versão ; a anterior continua protegida.
<code>sync --delete</code> e <code>rm --recursive</code>	Não apagam versões protegidas; apenas geram marcadores de exclusão.
Remover o bucket (<code>s3 rb</code>)	Falha enquanto existir qualquer versão protegida.
Modo GOVERNANCE com bypass	Permite excluir a versão ou reduzir a retenção, para quem tem a permissão específica.

BASH

```
# Somente em GOVERNANCE: excluir uma versão contornando a retenção
s3alt s3api delete-object --bucket empresa-imutavel --key contratos/c-001.pdf \
  --version-id <VERSION_ID> --bypass-governance-retention
```

ATENÇÃO Dados protegidos **continuam ocupando armazenamento** até o fim da retenção e não podem ser removidos antes disso para liberar espaço. Dimensione os prazos considerando o seu limite de armazenamento contratado.

8 Criptografia (SSE-S3)

Proteção dos dados em repouso com chaves gerenciadas pelo serviço

8.1 O que é e para que serve

A **criptografia no servidor** protege os seus arquivos **enquanto estão armazenados** (dados em repouso). O serviço oferece o **SSE-S3** (Server-Side Encryption com chaves gerenciadas pelo S3): cada objeto é criptografado com **AES-256** antes de ser gravado em disco e descriptografado automaticamente quando é baixado por quem tem permissão.

› Como funciona

- Você apenas indica que quer criptografar, em cada envio ou como padrão do bucket. **Não gera, guarda nem informa nenhuma chave.**
- As chaves são geradas, armazenadas e protegidas pelo próprio serviço.
- Nos downloads a descriptografia é transparente: os comandos continuam os mesmos.

› Para que serve

- Proteger os dados contra acesso indevido à mídia de armazenamento, como discos retirados, descartados ou lidos fora do serviço.
- Atender requisitos internos e de conformidade que exigem dados criptografados em repouso.
- Adotar criptografia **sem alterar** aplicações nem rotinas de backup.

NOTA A criptografia em repouso não substitui o controle de acesso: quem possui a access key e a secret key lê os dados normalmente, já descriptografados. Proteja as credenciais (seção 9).

8.2 Modalidades disponíveis

Modalidade	Como é solicitada	Disponibilidade
SSE-S3 (chaves gerenciadas pelo serviço)	<code>--sse AES256</code>	Disponível
SSE-KMS (chaves em um serviço KMS)	<code>--sse aws:kms</code>	Não disponível
SSE-C (chaves fornecidas pelo cliente)	<code>--sse-c</code> e <code>--sse-c-key</code>	Não disponível

ATENÇÃO Fornecemos **apenas SSE-S3**. Requisições com `--sse aws:kms` ou com chaves do cliente (SSE-C) retornam erro. Se você precisa controlar as próprias chaves, criptografe os arquivos **antes do envio** (criptografia no cliente): o serviço os armazena normalmente, e a guarda das chaves passa a ser inteiramente sua.

8.3 Ativar a criptografia padrão no bucket

Com a criptografia padrão ativa, **todo novo objeto** do bucket é criptografado com SSE-S3, mesmo que o envio não solicite criptografia. É a forma recomendada de uso.

BASH

```
s3alt s3api put-bucket-encryption --bucket empresa-backup \
--server-side-encryption-configuration '{
  "Rules": [ { "ApplyServerSideEncryptionByDefault": { "SSEAlgorithm": "AES256" } } ]
}'
```

BASH

```
# Consultar a configuração
s3alt s3api get-bucket-encryption --bucket empresa-backup

# Desativar a criptografia padrão (novos envios deixam de ser criptografados por padrão)
s3alt s3api delete-bucket-encryption --bucket empresa-backup
```

NOTA A criptografia padrão vale para os **novos** envios. Objetos que já estavam no bucket não são alterados; para criptografá-los, envie-os novamente com a criptografia padrão ativa.

DICA No PowerShell/Windows, grave o JSON em um arquivo (`sse.json`) e use `--server-side-encryption-configuration file://sse.json` .

8.4 Solicitar a criptografia em um envio

BASH

```
s3alt s3 cp ./dump.sql.gz s3://empresa-backup/2026/10/dump.sql.gz --sse AES256
s3alt s3 sync ./relatorios s3://empresa-backup/relatorios/ --sse AES256

s3alt s3api put-object --bucket empresa-backup --key doc.pdf --body ./doc.pdf \
--server-side-encryption AES256
```

8.5 Verificar se um objeto está criptografado

BASH

```
s3alt s3api head-object --bucket empresa-backup --key 2026/10/dump.sql.gz \
--query ServerSideEncryption
```

SAÍDA

```
"AES256"
```

Com a criptografia padrão ativa, objetos enviados sem `--sse` também retornam `AES256` .

8.6 Pontos de atenção

Tema	Orientação
Conexão segura	Use sempre HTTPS (o endpoint deste guia já usa). Pedidos de criptografia sem TLS são recusados.
Downloads e links	Nenhuma opção extra é necessária: <code>s3 cp</code> , <code>sync</code> e links <code>presign</code> funcionam normalmente.
Chaves	São gerenciadas pelo serviço: não é possível consultá-las, exportá-las nem rotacioná-las pelo CLI.
O que é criptografado	O conteúdo dos objetos. Nomes de objetos (chaves) e metadados não são criptografados: evite informações sensíveis em nomes de arquivos.
Object Lock	Pode ser combinada com Object Lock (seção 7): um bucket imutável também pode usar a criptografia padrão.

9 Boas práticas

Segurança das credenciais e uso no dia a dia

Prática	Como aplicar
Proteger os arquivos de credencial	<code>chmod 600 ~/.aws/credentials</code> ; nunca versionar a pasta <code>~/.aws</code> em Git.
Não compartilhar chaves	Cada sistema ou pessoa deve ter a sua credencial. Solicite credenciais adicionais ao suporte.
Não expor a secret	Não colar em chamados, e-mails, chats ou código-fonte. Em scripts, prefira <code>AWS_PROFILE</code> .
Trocar chaves periodicamente	Solicite a rotação ao suporte (ex.: a cada 90 dias) ou imediatamente em caso de suspeita de vazamento.
Simular antes de apagar	Use <code>--dryrun</code> em <code>rm --recursive</code> , <code>mv</code> e <code>sync --delete</code> .
Versionar dados críticos	Habilite o versionamento (seção 6) em buckets com dados importantes.
Proteger backups contra exclusão	Use Object Lock (seção 7) em buckets de backup. Comece em GOVERNANCE com prazo curto antes de adotar COMPLIANCE.
Criptografar dados em repouso	Ative a criptografia padrão SSE-S3 nos buckets (seção 8). É transparente para as aplicações.
Organizar por prefixos	Use chaves como <code>ano/mês/arquivo</code> para facilitar listagem, sincronização e limpeza.
Links temporários curtos	Em <code>presign</code> , use o menor prazo que atenda à necessidade.
Manter o CLI atualizado	Atualize periodicamente (seção 2.5).

9.1 Exemplo: backup diário agendado (Linux)

BASH

```
#!/usr/bin/env bash
# /usr/local/bin/backup-s3.sh
set -euo pipefail
export AWS_PROFILE=altatech
DATA=$(date +%Y/%m/%d)
aws s3 sync /srv/dados "s3://empresa-backup/diario/$DATA/" --only-show-errors
```

BASH

```
# crontab -e → executa todos os dias às 02:30
30 2 * * * /usr/local/bin/backup-s3.sh >> /var/log/backup-s3.log 2>&1
```

NOTA O agendamento roda com o usuário dono do crontab; o perfil `altatech` precisa estar configurado no `~/.aws` desse usuário.

10 Solução de problemas

Erros frequentes, causa provável e correção

Erro / sintoma	Causa provável	Correção
Could not connect to the endpoint URL	Endpoint digitado errado, sem internet ou bloqueio de firewall.	Conferir <code>endpoint_url</code> ; testar <code>curl -I https://s3.altatech.cloud</code> .
Comandos indo para amazonaws.com	CLI anterior à 2.13 ignora <code>endpoint_url</code> do perfil.	Atualizar o CLI (seção 2.5) ou usar <code>--endpoint-url</code> .
SSL: CERTIFICATE_VERIFY_FAILED	Data/hora errada ou certificados raiz do sistema desatualizados.	Ajustar o relógio; atualizar o pacote <code>ca-certificates</code> .
InvalidAccessKeyId	Access key digitada errada, desativada ou perfil errado.	<code>aws configure list --profile altatech</code> ; conferir variáveis <code>AWS_*</code> .
SignatureDoesNotMatch	Secret incorreta, espaço extra ou relógio fora de sincronia.	Regravar a secret; sincronizar o relógio (NTP).
AccessDenied	Credencial incorreta ou bucket que pertence a outro cliente.	Conferir <code>aws configure list</code> ; usar outro nome de bucket; contatar o suporte.
NoSuchBucket	Nome do bucket errado ou inexistente.	Conferir a grafia (só minúsculas).
NoSuchKey / 404	Caminho (chave) do objeto incorreto.	Listar o prefixo com <code>s3 ls</code> e copiar a chave exata.
InvalidLocationConstraint	Região do perfil diferente de <code>south-br-1</code> , ou placement digitado errado.	Conferir a região; para Object Lock usar exatamente <code>south-br-1:immutable-placement</code> (seção 7.3).
BucketAlreadyExists	Nome já usado.	Escolher outro nome (seção 4.2).
BucketNotEmpty	Bucket com objetos ou versões.	<code>s3 rb --force</code> ; se versionado, excluir versões (seção 6.5).
QuotaExceeded	Limite de armazenamento contratado atingido.	Liberar espaço (inclusive versões antigas) ou solicitar ampliação.
InvalidBucketState / InvalidRequest em comandos de lock	O bucket não foi criado com Object Lock.	Object Lock só pode ser habilitado na criação: crie um novo bucket (seção 7.3) e migre os dados.
AccessDenied ao excluir uma versão	Versão protegida por retenção ou legal hold.	Aguardar o fim da retenção; remover o legal hold; em GOVERNANCE, usar <code>--bypass-governance-retention</code> (seção 7.9).
InvalidArgument / NotImplemented com <code>--sse</code>	Uso de <code>aws:kms</code> ou de chaves do cliente (SSE-C).	Usar somente SSE-S3: <code>--sse AES256</code> (seção 8).
Erro de checksum / <code>InvalidArgument</code> no upload	Opções de checksum ausentes no CLI ≥ 2.23.	Configurar <code>request_checksum_calculation</code> e <code>response_checksum_validation</code> como <code>when_required</code> .

Erro / sintoma	Causa provável	Correção
Alias <code>s3alt</code> não funciona em script	Aliases não são lidos por scripts.	Usar <code>aws --profile altatech</code> ou <code>export AWS_PROFILE</code> .

10.1 Diagnóstico detalhado

BASH

```
# Mostra perfil, endpoint, região e a resposta completa do serviço
s3alt s3 ls s3://empresa-backup --debug 2>&1 | less

# Filtrar só o essencial
s3alt s3 ls s3://empresa-backup --debug 2>&1 | grep -E "endpoint|Response|Error|status"
```

DICA Ao abrir um chamado, envie o comando executado e a mensagem de erro. **Nunca** envie a secret key nem o conteúdo de `~/.aws/credentials`; a saída de `--debug` não exibe a secret.

11 Referência rápida

Os comandos do guia em uma página

Área	Operação	Comando
Instalação	Versão instalada	<code>aws --version</code>
Perfil	Criar perfil	<code>aws configure --profile altatech</code>
Perfil	Definir endpoint	<code>aws configure set endpoint_url https://s3.altatech.cloud --profile altatech</code>
Perfil	Ver configuração	<code>aws configure list --profile altatech</code>
Bucket	Criar	<code>s3alt s3 mb s3://<bucket></code>
Bucket	Listar buckets	<code>s3alt s3 ls</code>
Bucket	Listar conteúdo	<code>s3alt s3 ls s3://<bucket>/<prefixo>/</code>
Bucket	Espaço utilizado	<code>s3alt s3 ls s3://<bucket> --recursive --human-readable --summarize</code>
Bucket	Remover	<code>s3alt s3 rb s3://<bucket> [--force]</code>
Objeto	Enviar	<code>s3alt s3 cp <arquivo> s3://<bucket>/<chave></code>
Objeto	Baixar	<code>s3alt s3 cp s3://<bucket>/<chave> <arquivo></code>
Objeto	Diretório inteiro	<code>s3alt s3 cp <dir> s3://<bucket>/<prefixo>/ --recursive</code>
Objeto	Sincronizar	<code>s3alt s3 sync <dir> s3://<bucket>/<prefixo>/ [--delete] [--dryrun]</code>
Objeto	Mover / renomear	<code>s3alt s3 mv s3://<bucket>/<a> s3://<bucket>/</code>
Objeto	Excluir	<code>s3alt s3 rm s3://<bucket>/<chave> [--recursive]</code>
Objeto	Detalhes	<code>s3alt s3api head-object --bucket <bucket> --key <chave></code>
Objeto	Link temporário	<code>s3alt s3 presign s3://<bucket>/<chave> --expires-in 3600</code>
Versões	Habilitar	<code>s3alt s3api put-bucket-versioning --bucket --versioning-configuration Status=Enabled</code>
Versões	Listar	<code>s3alt s3api list-object-versions --bucket --prefix <chave></code>
Versões	Baixar versão	<code>s3alt s3api get-object --bucket --key <chave> --version-id <id> <arquivo></code>
Versões	Desfazer exclusão	<code>s3alt s3api delete-object --bucket --key <chave> --version-id <id-do-marcador></code>
Object Lock	Criar bucket	<code>s3alt s3api create-bucket --bucket --object-lock-enabled-for-bucket --create-bucket-configuration LocationConstraint=south-br-1:immutable-placement</code>
Object Lock	Retenção padrão	<code>s3alt s3api put-object-lock-configuration --bucket --object-lock-configuration '<JSON>' (seção 7.5)</code>

Área	Operação	Comando
Object Lock	Retenção por versão	s3alt s3api put-object-retention --bucket --key <chave> --version-id <id> --retention Mode=COMPLIANCE,RetainUntilDate=<data>
Object Lock	Legal hold	s3alt s3api put-object-legal-hold --bucket --key <chave> --legal-hold Status=ON
Criptografia	Padrão no bucket	s3alt s3api put-bucket-encryption --bucket --server-side-encryption-configuration '<JSON>' (seção 8.3)
Criptografia	Por envio	s3alt s3 cp <arquivo> s3://<bucket>/<chave> --sse AES256
Criptografia	Verificar	s3alt s3api head-object --bucket --key <chave> --query ServerSideEncryption
Diagnóstico	Depurar	<comando> --debug