aws

Guia do usuário

Amazon S3 on Outposts

Versão da API 2006-03-01

Amazon S3 on Outposts: Guia do usuário

Table of Contents

O que é o S3 on Outposts? ... 1
Como funciona o S3 on Outposts ... 1
Regiões ... 2
Buckets ... 2
Objetos ... 3
Chaves ... 3
Versionamento do S3 ... 4
ID da versão ... 4
Classe de armazenamento e criptografia ... 4
Política de bucket ... 5
Pontos de acesso do S3 on Outposts ... 5
Recursos do S3 on Outposts ... 6
Gerenciamento de acesso ... 6
Registro e monitoramento do armazenamento ... 7
Consistência forte ... 7
Serviços relacionados ... 7
Acessar o S3 no Outposts ... 8
Console de gerenciamento da AWS ... 8
AWS Command Line Interface ... 8
AWS SDKs ... 8
Pagar pelo S3 on Outposts ... 9
Próximas etapas ... 9
Configurar seu Outpost ... 10
Pedir um novo Outpost ... 10
Em que aspectos o S3 on Outposts é diferente? ... 11
Especificações ... 11
Operações de API compatíveis ... 12
Comandos da AWS CLI do Amazon S3 compatíveis com o S3 no Outposts ... 12
Recursos não compatíveis do Amazon S3 ... 12
Restrições de rede ... 13
Conceitos básicos do S3 no Outposts ... 15
Usar o console do S3 ... 15
Criar um bucket, um ponto de acesso e um endpoint ... 16
Próximas etapas ... 18

Usar a AWS CLI e o SDK para Java ... 19
Etapa 1: Criar um bucket ... 19
Etapa 2: Criar um ponto de acesso ... 20
Etapa 3: Criar um endpoint ... 21
Etapa 4: Fazer upload de um objeto em um bucket do S3 on Outposts ... 22
Redes para S3 on Outposts ... 23
Escolher seu tipo de acesso às redes ... 23
Acessar buckets e objetos do S3 on Outposts ... 23
Gerenciar conexões usando interfaces de rede elástica entre contas ... 24
Trabalhar com buckets do S3 on Outposts ... 25
Buckets ... 25
Pontos de acesso ... 25
Endpoints ... 26
Operações de API no S3 on Outposts ... 26
Criar e gerenciar o bucket do S3 no Outposts ... 28
Como criar um bucket ... 28
Adicionar etiquetas ... 32
Uso de políticas de bucket ... 34
Adicionar uma política de bucket ... 34
Visualizar uma política de bucket ... 37
Excluir uma política de bucket ... 38
Exemplos de políticas de bucket ... 39
Listar buckets ... 43
Obter um bucket ... 45
Excluir bucket ... 46
Trabalhar com pontos de acesso ... 48
Criar um ponto de acesso ... 48
Usar um alias em estilo de bucket para seu ponto de acesso ... 50
Exibir a configuração do ponto de acesso ... 54
Listar pontos de acesso ... 55
Excluir um ponto de acesso ... 57
Adicionar uma política de ponto de acesso ... 57
Visualizar uma política de ponto de acesso ... 60
Trabalhar com endpoints do ... 61
Criar um endpoint ... 62
Listar endpoints ... 64

Excluir um endpoint ... 66
Trabalhar com objetos usando o S3 on Outposts ... 68
Fazer upload de um objeto ... 69
Copiar um objeto ... 70
Usar o AWS SDK para Java ... 71
Obter um objeto ... 72
Listar objetos ... 75
Excluir objetos ... 78
Usar o HeadBucket ... 83
Executar um carregamento fracionado ... 85
Efetuar o upload fracionado de um objeto em um bucket do Amazon S3 on Outposts ... 85
Copiar um objeto grande em um bucket do S3 on Outposts usando carregamento fracionado ... 88
Listar partes de um objeto em um bucket do S3 no Outposts ... 90
Recuperar uma lista de multipart uploads em andamento em um bucket do S3 no Outposts ... 91
Usar pre-signed URLs ... 92
Limitar recursos de pre-signed URLs ... 93
Quem pode criar um URL pré-assinado ... 95
Quando o S3 no Outposts confere a data e a hora de validade de um URL pré-assinado? ... 96
Compartilhar objetos ... 96
Fazer upload de um objeto ... 101
Amazon S3 no Outposts com Amazon EMR local ... 106
Criar um bucket do Amazon S3 no Outposts ... 107
Conceitos básicos do Amazon EMR com o Amazon S3 no Outposts ... 108
Armazenamento em cache de autorização e autenticação ... 113
Configurar o cache de autorização e autenticação ... 114
Validar a assinatura do SigV4A ... 114
Segurança ... 115
Configurar o IAM ... 116
Entidades principais para S3 no Outposts ... 118
ARNs para S3 no Outposts ... 118
Exemplo de políticas para S3 no Outposts ... 120
Permissões para endpoints ... 120
Perfis vinculados a serviço para o S3 no Outposts ... 123
Criptografia de dados ... 123

AWS PrivateLink para S3 on Outposts 123
Restrições e limitações 125
Acessar endpoints da interface do S3 on Outposts 125
Atualizar uma configuração de DNS on-premises 127
Criar um endpoint da VPC 127
Criar políticas de bucket e políticas de endpoint da VPC 127
Chaves de política do Signature Version 4 (SigV4) 130
Exemplos de política de bucket que usam chaves de condição relacionadas ao Signature Version 4 132
Políticas gerenciadas pela AWS 135
AWSS3OnOutpostsServiceRolePolicy 135
Atualizações da política 135
Uso de perfis vinculados ao serviço 136
Permissões de perfil vinculado a serviço para o S3 no Outposts 136
Criar um perfil vinculado a serviço para o S3 no Outposts 139
Editar um perfil vinculado a serviço para o S3 no Outposts 140
Excluir um perfil vinculado a serviço para o S3 no Outposts 140
Regiões compatíveis com perfis vinculados a serviço do S3 no Outposts 141
Gerenciar o armazenamento do S3 on Outposts 142
Gerenciar o versionamento do S3 142
Criar e gerenciar uma configuração de ciclo de vida 145
Utilizar o console 145
Usar a AWS CLI e o SDK para Java 150
Replicar objetos para o S3 no Outposts 154
Configuração de replicação 154
Requisitos para a replicação do S3 no Outposts 155
O que é replicado? 156
O que não é replicado? 157
O que não é compatível com a replicação do S3 no Outposts? 158
Configuração da replicação 158
Gerenciar sua replicação 178
Compartilhar o S3 on Outposts 186
Pré-requisitos 187
Procedimento 187
Exemplos de uso 188
Outros produtos da 191

Monitoramento do S3 on Outposts 192
Métricas do CloudWatch 192
Métricas do CloudWatch 193
Amazon CloudWatch Events 195
Logs do CloudTrail 196
Habilitar o registro em log do CloudTrail para objetos do S3 no Outposts 197
Entradas de arquivo de log do AWS CloudTrail do Amazon S3 no Outposts 199
Desenvolver com o S3 on Outposts 202
Regiões compatíveis 202
APIs do S3 on Outposts 203
Operações de API do Amazon S3 para gerenciar objetos 203
Operações de API do Amazon S3 Control para gerenciar buckets 204
Operações de API do S3 on Outposts para gerenciar Outposts 205
Configurar o cliente de controle do S3 206
Fazer solicitações por meio do IPv6 206
Conceitos básicos do IPv6 207
Fazer solicitações usando endpoints de pilha dupla 208
Como usar endereços do IPv6 em políticas do IAM 208
Testar a compatibilidade com endereços IP 210
Usar IPv6 com o AWS PrivateLink 210
Usar endpoints de pilha dupla 213

O que é o Amazon S3 on Outposts?

O AWS Outposts é um serviço totalmente gerenciado que oferece a mesma infraestrutura da AWS, APIs, ferramentas e serviços da AWS, para praticamente qualquer datacenter, espaço de colocalização ou instalação on-premises para uma experiência híbrida verdadeiramente consistente. O AWS Outposts é ideal para workloads que exigem acesso de baixa latência a sistemas on-premises, processamento de dados local, residência de dados e migração de aplicações com interdependências do sistema local. Para obter mais informações, consulte O que é o AWS Outposts? no Guia do usuário do AWS Outposts.

Com o Amazon S3 no Outposts, você pode criar buckets do S3 em seu Outposts, além de armazenar e recuperar objetos facilmente on-premises. O S3 no Outposts fornece uma nova classe de armazenamento, `OUTPOSTS`, que usa as APIs do Amazon S3 e é projetada para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC).

É possível usar as mesmas APIs e recursos nos buckets do Outposts da mesma maneira que no Amazon S3, como políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST.

- Como funciona o S3 on Outposts
- Recursos do S3 on Outposts
- Serviços relacionados
- Acessar o S3 no Outposts
- Pagar pelo S3 on Outposts
- Próximas etapas

Como funciona o S3 on Outposts

O S3 on Outposts é um serviço de armazenamento de objetos que armazena dados como objetos em buckets em seu Outpost. Objeto é um arquivo de dados e quaisquer metadados que descrevam o arquivo. Um bucket é um contêiner de objetos.

Para armazenar seus dados no S3 on Outposts, primeiro crie um bucket. Ao criar o bucket, especifique um nome para ele e o Outpost que o conterá. Para acessar o bucket do S3 on Outposts e executar operações de objeto, em seguida você vai criar e configurar um ponto de acesso. Você também deve criar um endpoint para encaminhar solicitações para seu ponto de acesso.

Os pontos de acesso simplificam o acesso a dados para qualquer AWS service (Serviço da AWS) ou aplicação de cliente que armazene dados no S3. Os pontos de acesso são endpoints de rede nomeados que são anexados a buckets e podem ser usados para executar operações de objeto, como `GetObject` e `PutObject`. Cada ponto de acesso tem permissões e controles de rede distintos.

Você pode criar e gerenciar seus buckets, pontos de acesso e endpoints do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS CLI, AWS SDKs ou a API REST. Para carregar e gerenciar objetos no bucket do S3 on Outposts, é possível usar a AWS CLI, AWS SDKs ou a API REST.

Regiões

Durante o provisionamento AWS Outposts, você ou a AWS cria uma conexão de link de serviço que conecta seu Outpost de volta à Região da AWS escolhida ou à região inicial do Outposts para operações de bucket e telemetria. Um Outpost depende da conectividade com a principal Região da AWS. O rack Outposts não foi projetado para operações ou ambientes desconectados com pouca ou nenhuma conectividade. Para obter mais informações, consulte Conectividade do Outpost com as Regiões da AWS no Manual do usuário do AWS Outposts.

Buckets

Bucket é um contêiner para objetos armazenados no S3 on Outposts. Você pode armazenar qualquer número de objetos em um bucket e ter até 100 buckets por conta e Outpost.

Ao criar um bucket, você insere um nome para ele e escolhe o Outpost onde ele residirá. Assim que você cria um bucket, não pode mais alterar o respectivo nome nem o mover para outro Outpost. Os nomes de buckets devem seguir as regras de nomenclatura de buckets do Amazon S3. No S3 on Outposts, os nomes de bucket são exclusivos de um Outpost e de uma Conta da AWS. Os buckets do S3 on Outposts exigem o `outpost-id`, o `account-id` e o nome do bucket para identificá-los.

O exemplo a seguir mostra o formato do nome do recurso da Amazon (ARN) para buckets do S3 no Outposts. O ARN é composto da região na qual o Outpost está hospedado, de sua conta do Outpost, do ID do Outpost e do nome do bucket.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/bucket-name
```

Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Ao especificar o bucket para operações de objeto, use o ARN do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN de ponto de acesso do S3 no Outposts, que inclui o `outpost-id`, o `account-id` e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre buckets, consulte Trabalhar com buckets do S3 on Outposts.

Objetos

Os objetos são as entidades fundamentais armazenadas no S3 on Outposts. Os objetos consistem em metadados e dados de objeto. Os metadados são um conjunto de pares de nome e valor que descrevem o objeto. Esses pares incluem alguns metadados padrão, como a data da última modificação, e metadados HTTP padrão, como o `Content-Type`. Você também pode especificar metadados personalizados no momento em que o objeto é armazenado. Um objeto é identificado exclusivamente em um bucket por uma chave (ou nome).

Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Chaves

Uma chave de objeto (ou nome da chave) é um identificador exclusivo de um objeto em um bucket. Cada objeto em um bucket tem exatamente uma chave. A combinação de um bucket e uma chave de objeto identifica exclusivamente cada objeto.

O exemplo a seguir mostra o formato do ARN para objetos do S3 on Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost, o nome do bucket e a chave de objeto:

```
arn:aws:s3-outposts:us-west-2:123456789012:outpost/ op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1/object/myobject
```

Para obter mais informações sobre chaves de objeto, consulte Trabalhar com objetos usando o S3 on Outposts.

Versionamento do S3

Use o versionamento do S3 em buckets do Outposts para manter diversas variantes de um objeto no mesmo bucket. Com o versionamento do S3, você pode preservar, recuperar e restaurar todas as versões de cada objeto armazenado em seus buckets. O versionamento do S3 ajuda você a se recuperar de ações não intencionais de usuários e de falhas da aplicação.

Para obter mais informações, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.

ID da versão

Se você habilitar o versionamento do S3 em um bucket, o S3 no Outposts gerará um ID de versão exclusivo para cada objeto adicionado ao bucket. Os objetos que já existiam no bucket no momento em que você habilita o controle de versão têm um ID de versão `null`. Se você modificar esses (ou quaisquer outros) objetos com outras operações, como PutObject, os novos objetos receberão um ID de versão exclusivo.

Para obter mais informações, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.

Classe de armazenamento e criptografia

O S3 no Outposts fornece uma nova classe de armazenamento, o S3 Outposts (`OUTPOSTS`). A classe de armazenamento do S3 Outposts só está disponível para objetos armazenados em buckets no AWS Outposts. Se você tentar usar outras classes de armazenamento do S3 com o S3 on Outposts, o S3 on Outposts retornará o erro `InvalidStorageClass`.

Por padrão, os objetos armazenados na classe de armazenamento S3 Outposts (`OUTPOSTS`) são sempre criptografados usando criptografia no lado do servidor com chaves de criptografia

gerenciadas pelo Amazon S3 (SSE-S3). Para obter mais informações, consulte Criptografia de dados no S3 on Outposts.

Política de bucket

Uma política de bucket é baseada em recursos do AWS Identity and Access Management (IAM) que você pode usar para conceder permissões de acesso ao bucket e aos objetos nele contidos. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. As políticas de bucket são limitadas a 20 KB.

As políticas de bucket usam uma linguagem de política do IAM baseadas em JSON que é padrão na AWS. Você pode usar políticas de bucket para adicionar ou negar permissões para os objetos em um bucket. As políticas de bucket permitem ou negam solicitações com base nos elementos da política. Esses elementos podem incluir o solicitante, ações do S3 on Outposts, recursos e aspectos ou condições da solicitação (por exemplo, o endereço IP usado para fazer a solicitação). Por exemplo, você pode criar uma política de bucket que conceda permissões entre contas para carregar objetos em um bucket do S3 on Outposts e garantir que o proprietário do bucket tenha controle total sobre os objetos carregados.

Na política de bucket, você pode usar caracteres curinga (`*`) nos ARNs e outros valores para conceder permissões a um subconjunto de objetos. Por exemplo, você pode controlar o acesso a grupos de objetos que começam com um prefixo ou termine com uma determinada extensão, como `.html`.

Pontos de acesso do S3 on Outposts

Os pontos de acesso do Amazon S3 são endpoints de rede nomeados com políticas de acesso dedicadas que descrevem como os dados podem ser acessados usando esse endpoint. Os pontos de acesso simplificam o gerenciamento de acesso a dados em escala para conjuntos de dados compartilhados no S3 on Outposts. Os pontos de acesso são anexados a buckets que você pode usar para executar operações de objeto do S3, como `GetObject` e `PutObject`.

Ao especificar o bucket para operações de objeto, use o ARN do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

Cada ponto de acesso tem permissões distintas e controles de rede que o S3 on Outposts aplica para qualquer solicitação feita por meio desse ponto de acesso. Cada ponto de acesso impõe

uma política de ponto de acesso personalizada que funciona em conjunto com a política de bucket anexada ao bucket subjacente.

Para obter mais informações, consulte Acessar buckets e objetos do S3 on Outposts.

Recursos do S3 on Outposts

Gerenciamento de acesso

O S3 on Outposts fornece recursos para auditoria e gerenciamento de acesso a seus buckets e objetos. Por padrão, os buckets do S3 on Outposts e os objetos que eles contêm são privados. Você tem acesso somente aos recursos do S3 on Outposts criados por você.

Para conceder permissões de recursos detalhadas que sejam compatíveis com seu caso de uso específico ou para auditar as permissões de seus recursos do S3 on Outposts, você pode usar os recursos a seguir.

- Bloqueio de acesso público do S3: bloqueie o acesso público a buckets e objetos. Para buckets no Outposts, a opção Block Public Acces (Bloquear acesso público) está sempre habilitada por padrão.
- AWS Identity and Access Management (IAM): o IAM é um serviço da Web que ajuda você a controlar de maneira segura o acesso aos recursos da AWS, incluindo seus recursos do S3 no Outposts. Com o IAM, é possível gerenciar, de maneira centralizada, permissões que controlam quais recursos da AWS os usuários poderão acessar. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) para usar os recursos.
- Pontos de acesso do S3 on Outposts: gerencie o acesso a dados para conjuntos de dados compartilhados no S3 on Outposts. Os pontos de acesso são endpoints de rede nomeados com políticas de acesso dedicadas. Os pontos de acesso são anexados a buckets e podem ser usados para executar operações de objeto, como `GetObject` e `PutObject`.
- Políticas de buckets: use a linguagem de política baseada em IAM para configurar permissões baseadas em recursos para os buckets do S3 e os objetos neles contidos.
- AWS Resource Access Manager(AWS RAM): compartilhe com segurança a capacidade do S3 on Outposts com Contas da AWS, dentro de sua organização ou unidades organizacionais (OUs) no AWS Organizations.

Registro e monitoramento do armazenamento

O S3 on Outposts fornece ferramentas de registro em log e monitoramento que você pode usar para monitorar e controlar como seus recursos do S3 on Outposts estão sendo usados. Para obter mais informações, consulte Ferramentas de monitoramento.

- Métricas do Amazon CloudWatch para o S3 on Outposts: monitore a integridade operacional de seus recursos e conheça sua disponibilidade de capacidade.
- Eventos do Amazon CloudWatch Events para o S3 on Outposts: crie uma regra para qualquer evento da API do S3 on Outposts para receber notificações por meio de todos os destinos compatíveis do CloudWatch Events, incluindo o Amazon Simple Queue Service (Amazon SQS), o Amazon Simple Notification Service (Amazon SNS) e o AWS Lambda.
- Logs do AWS CloudTrail para o S3 on Outposts: registre ações executadas por um usuário, uma função ou um AWS service (Serviço da AWS) no S3 on Outposts. Os logs do CloudTrail fornecem rastreamento detalhado de API para operações no nível de bucket e objeto do S3.

Consistência forte

O S3 on Outposts oferece uma sólida consistência de leitura após gravação para solicitações PUT e DELETE de objetos no bucket do S3 on Outposts em todas as Regiões da AWS. Esse comportamento se aplica a ambas as gravações em novos objetos, bem como a solicitações PUT que substituem objetos existentes e a solicitações DELETE. Além disso, as etiquetas de objeto e os metadados de objeto do S3 on Outposts (por exemplo, objeto HEAD) são fortemente consistentes. Consulte mais informações em Modelo de consistência de dados do Amazon S3 no Guia do usuário do Amazon S3.

Serviços relacionados

Depois de carregar os dados no S3 on Outposts, você poderá usá-los com outros Serviços da AWS. Os serviços a seguir podem ser usados com mais frequência:

- Amazon Elastic Compute Cloud (Amazon EC2): oferece capacidade de computação escalável na Nuvem AWS. O uso do Amazon EC2 reduz a necessidade de investimento antecipado em hardware. Por isso, você pode desenvolver e implantar aplicações com maior rapidez. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento.

- Amazon Elastic Block Store (Amazon EBS) on Outposts: use snapshots locais do Amazon EBS no Outposts para armazenar snapshots de volumes localmente em um Outpost no S3 on Outposts.
- Amazon Relational Database Service (Amazon RDS) on Outposts: use backups locais do Amazon RDS para armazenar seus backups do Amazon RDS localmente em seu Outpost.
- AWS DataSync: automatize a transferência de dados entre os Outposts e as Regiões da AWS, escolhendo o que transferir, quando transferir e a quantidade de largura de banda de rede a ser usada. O S3 no Outposts é integrado ao AWS DataSync. Para aplicativos locais que exigem processamento local de alto rendimento, o S3 on Outposts fornece armazenamento de objetos no local para minimizar transferências de dados e buffer de variações de rede, ao mesmo tempo que oferece a você a capacidade de transferir dados facilmente entre Outposts e Regiões da AWS.

Acessar o S3 no Outposts

Você pode trabalhar com o S3 on Outposts de uma das seguintes formas:

Console de gerenciamento da AWS

O console é uma interface de usuário baseada na Web para gerenciar o S3 on Outposts e o recursos da AWS. Se você se cadastrou em uma Conta da AWS, pode acessar o S3 on Outposts fazendo login no Console de gerenciamento da AWS e escolhendo S3 na página inicial do Console de gerenciamento da AWS. Depois, escolha Outposts buckets (Buckets do Outposts) no painel de navegação à esquerda.

AWS Command Line Interface

Você pode usar as ferramentas de linha de comando da AWS para emitir comandos ou criar scripts na linha de comando de seu sistema e executar tarefas da AWS (incluindo o S3).

A AWS Command Line Interface (AWS CLI) fornece comandos para um amplo conjunto de Serviços da AWS. A AWS CLI é compatível com Windows, macOS e Linux. Para começar a usar, consulte o Guia do usuário da AWS Command Line Interface. Para obter mais informações sobre os comandos que você pode usar com o S3 on Outposts, consulte s3api, s3control e s3outposts na Referência de comando da AWS CLI.

AWS SDKs

AWSA fornece SDKs (kits de desenvolvimento de software) que consistem em bibliotecas e códigos de exemplo para várias linguagens de programação e plataformas (Java, Python, Ruby, .NET, iOS,

Android etc.). Os AWS SDKs são uma forma conveniente de criar acesso programático para o S3 on Outposts e a AWS. Como o S3 on Outposts usa os mesmos SDKs do Amazon S3, o S3 on Outposts oferece uma experiência consistente usando a mesma automação e as mesmas APIs e ferramentas do S3.

O S3 on Outposts é um serviço REST. Você pode enviar solicitações para o S3 on Outposts usando bibliotecas do AWS SDK que envolvem a API REST subjacente e simplificam as tarefas de programação. Por exemplo, os SDKs processam tarefas como calcular assinaturas, assinar solicitações de forma criptográfica, gerenciar erros e novas tentativas automáticas de solicitações. Para obter informações sobre os AWS SDKs, inclusive sobre como baixá-los e instalá-los, consulte Aprenda a criar na AWS.

Pagar pelo S3 on Outposts

Você pode comprar uma variedade de configurações de rack do AWS Outposts, que oferecem uma combinação de tipos de instância do Amazon EC2, volumes de unidade de estado sólido (SSD) de uso geral (SSD) do Amazon EBS (gp2) e o S3 on Outposts. O preço inclui entrega, instalação e manutenção do serviço de infraestrutura, bem como patches e atualizações de software.

Para obter mais informações, consulte Preços de rack AWS Outposts.

Próximas etapas

Para obter mais informações sobre como trabalhar com o S3 on Outposts, consulte os seguintes tópicos:

- Configurar seu Outpost
- O Amazon S3 on Outposts é diferente do Amazon S3?
- Conceitos básicos do Amazon S3 on Outposts
- Redes para S3 on Outposts
- Trabalhar com buckets do S3 on Outposts
- Trabalhar com objetos usando o S3 on Outposts
- Segurança no S3 on Outposts
- Gerenciar o armazenamento do S3 on Outposts
- Desenvolver com o Amazon S3 on Outposts

Configurar seu Outpost

Para começar a usar o Amazon S3 on Outposts, você precisa de um Outpost com capacidade do Amazon S3 implantada em suas instalações. Para obter informações sobre opções para solicitar um Outpost e capacidade do S3, consulte AWS Outposts. Para verificar se o Outposts tem capacidade do S3, você pode usar a chamada de API ListOutpostsWithS3. Para obter especificações e ver como o S3 on Outposts é diferente do Amazon S3, consulte . O Amazon S3 on Outposts é diferente do Amazon S3?

Para obter mais informações, consulte os tópicos a seguir.

Tópicos

- Pedir um novo Outpost

Pedir um novo Outpost

Se precisar solicitar um novo Outpost com capacidade do S3, consulte Preços de racks do AWS Outposts para entender a opção de capacidade do Amazon Elastic Compute Cloud (Amazon EC2), do Amazon Elastic Block Store (Amazon EBS) e do Amazon S3

Depois de selecionar a configuração, siga as etapas em Create an Outpost and order Outpost capacity (Criar um Outpost e solicitar capacidade do Outpost) no Guia do usuário do AWS Outposts.

O Amazon S3 on Outposts é diferente do Amazon S3?

O Amazon S3 no Outposts fornece armazenamento de objetos para seu ambiente do AWS Outposts on-premises. Usar o S3 no Outposts ajuda você a atender às necessidades de processamento local, residência de dados e alto nível de performance, mantendo os dados próximos às aplicações on-premises. Como ele usa APIs e recursos do Amazon S3, o S3 no Outposts facilita o armazenamento, a proteção, a etiquetagem, a geração de relatórios e o controle de acesso aos dados em seus Outposts, bem como a extensão da infraestrutura da AWS para suas instalações on-premises a fim de oferecer uma experiência híbrida consistente.

Para obter mais informações sobre os aspectos que diferenciam o S3 on Outposts, consulte os tópicos a seguir.

Tópicos

- Especificações do Amazon S3 no Outposts
- Operações de API compatíveis com o Amazon S3 no Outposts
- Comandos da AWS CLI do Amazon S3 compatíveis com o S3 no Outposts
- Recursos do Amazon S3 não compatíveis com o S3 no Outposts.
- Requisitos de rede do S3 on Outposts

Especificações do Amazon S3 no Outposts

- O tamanho máximo do bucket do Outposts é de 50 TB.
- O tamanho máximo de objeto é 5 TB em buckets do Outposts.
- O número máximo de buckets de Outposts é 100 por Conta da AWS.
- Os buckets do Outposts só podem ser acessados usando pontos de acesso e endpoints.
- O número máximo de pontos de acesso por bucket de Outposts é dez.
- As políticas de ponto de acesso estão limitadas a 20 KB.
- O proprietário do Outpost pode gerenciar o acesso dentro de sua organização no AWS Organizations usando o AWS Resource Access Manager. Todas as contas que precisam de acesso ao Outpost devem estar dentro da mesma organização que a conta de proprietário no AWS Organizations.
- A conta de proprietário do bucket do S3 on Outposts é sempre o proprietário de todos os objetos no bucket.

- Somente a conta de proprietário do bucket do S3 no Outposts pode executar operações no bucket.
- As limitações de tamanho do objeto são consistentes com o Amazon S3.
- Todos os objetos armazenados no S3 no Outposts são armazenados na classe de armazenamento do `OUTPOSTS`.
- Por padrão, todos os objetos armazenados na classe de armazenamento `OUTPOSTS` são armazenados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Você também pode optar explicitamente por armazenar objetos usando a criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C).
- Se não houver espaço suficiente para armazenar um objeto em seu Outpost, a API retornará uma exceção de capacidade insuficiente (ICE).

Operações de API compatíveis com o Amazon S3 no Outposts

Para obter uma lista das operações de API compatíveis com o S3 on Outposts, consulte Operações de API do Amazon S3 on Outposts.

Comandos da AWS CLI do Amazon S3 compatíveis com o S3 no Outposts

Os comandos da AWS CLI do Amazon S3 a seguir agora são compatíveis com o Amazon S3 no Outposts. Para obter mais informações, consulte Available Commands na Referência de comandos da AWS CLI.

- `cp`, `mv` e `sync` dentro do mesmo bucket do Outposts ou entre um ambiente local e um bucket do Outposts.
- `ls`
- `presign`
- `rm`

Recursos do Amazon S3 não compatíveis com o S3 no Outposts.

Os recursos do Amazon S3 a seguir não são compatíveis com o Amazon S3 on Outposts. Todas as tentativas de usá-los são rejeitadas.

- Solicitações condicionais
- Listas de controle de acesso (ACLs)
- Compartilhamento de recursos de origem cruzada (CORS)
- Operações em lote do S3
- Relatórios de inventário do S3
- Alterar a criptografia de bucket padrão
- Buckets públicos
- Exclusão de autenticação multifator (MFA)
- Transições do ciclo de vida do S3 (além da exclusão de objetos e da interrupção de carregamentos fracionados incompletos)
- Retenção legal do Bloqueio de objetos do S3
- Retenção do Bloqueio de objetos
- Criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS)
- Controle do tempo de replicação do S3 (S3 RTC)
- Métricas de solicitação do Amazon CloudWatch
- Configuração de métricas
- Transfer Acceleration
- Notificações de eventos do S3
- Buckets de pagamento pelo solicitante
- S3 Select
- AWS LambdaEventos do
- Server access logging (Registro em log de acesso ao servidor)
- Solicitações HTTP POST
- SOAP
- Acesso ao site

Requisitos de rede do S3 on Outposts

- Para rotear solicitações para um ponto de acesso do S3 no Outposts, você deve criar e configurar um endpoint do S3 no Outposts. Os seguintes limites se aplicam aos endpoints do S3 no Outposts:

  - Cada nuvem privada virtual (VPC) em um Outpost pode ter um endpoint associado e é possível ter até 100 endpoints por Outpost.
  - É possível mapear vários pontos de acesso para o mesmo endpoint.
  - Você só pode adicionar endpoints a VPCs com blocos CIDR nos subespaços dos seguintes intervalos CIDR:
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
- Você só pode criar endpoints para um Outpost de VPCs que tenham blocos CIDR não sobrepostos.
- Só é possível criar um endpoint de sua própria sub-rede de Outposts.
- A sub-rede utilizada para criar um endpoint deve conter quatro endereços IP para uso do S3 on Outposts.
- Se você especificar o grupo de endereços IP de propriedade do cliente (grupo de CoIP), ele deverá conter quatro endereços IP para uso do S3 on Outposts.
- Só é possível criar um endpoint por Outpost por VPC.

Conceitos básicos do Amazon S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (OUTPOSTS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST.

Com o Amazon S3 on Outposts, você pode usar as APIs e recursos do Amazon S3, como armazenamento de objetos, políticas de acesso, criptografia e marcação, no AWS Outposts da mesma forma que no Amazon S3. Para obter informações sobre o S3 on Outposts, consulte O que é o Amazon S3 on Outposts?.

Tópicos

- Conceitos básicos do uso do Console de gerenciamento da AWS
- Como começar a usar a AWS CLI e o SDK para Java

Conceitos básicos do uso do Console de gerenciamento da AWS

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (OUTPOSTS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Para começar a usar o S3 on Outposts utilizando o console, consulte os tópicos a seguir. Para começar a usar a AWS CLI ou o AWS SDK para Java, consulte.

Tópicos

- Criar um bucket, um ponto de acesso e um endpoint
- Próximas etapas

Criar um bucket, um ponto de acesso e um endpoint

O procedimento a seguir mostra como criar seu primeiro bucket no S3 on Outposts. Ao criar um bucket pela primeira vez usando o console, você também cria um ponto de acesso e um endpoint associados ao bucket para que possa começar a armazenar objetos no bucket imediatamente.

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha Create Outposts bucket (Criar bucket do Outposts).
4. Em Bucket name (Nome do bucket), insira um nome compatível com o Sistema de Nome de Domínio (DNS) para seu bucket.

   O nome do bucket deve:

   - Ser único dentro da Conta da AWS, do Outpost e da Região da AWS na qual o Outpost está alojado.
   - Ter entre 3 e 63 caracteres.
   - Não contém caracteres maiúsculos.
   - Começar com uma letra minúscula ou um número.

   Depois de criado o bucket, você não pode mudar seu nome. Consulte informações sobre como nomear buckets em Regras de nomenclatura de buckets de diretório no Guia do usuário do Amazon S3.

   > **Important**
   >
   > Evite incluir informações confidenciais, como números de conta, no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

5. Em Outpost, escolha o Outpost onde você quer que o bucket resida.
6. Em Bucket Versioning (Versionamento de bucket), defina o estado de versionamento do S3 para seu bucket do S3 no Outposts como uma das seguintes opções:

   - Disable (Desabilitar) (padrão): o bucket permanece sem versão.
   - Enable (Habilitar): habilita o versionamento do S3 para os objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo.

   Para obter mais informações sobre o S3 Versioning, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.
7. (Opcional) Adicione as optional tags (etiquetas opcionais) que você gostaria de associar ao bucket do Outposts. Você pode usar etiquetas para monitorar os critérios para projetos específicos ou grupos de projetos ou para rotular seus buckets usando etiquetas de alocação de custo.

   Por padrão, todos os objetos armazenados no bucket do Outposts são armazenados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Você também pode optar explicitamente por armazenar objetos usando a criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C). Para alterar o tipo de criptografia, você deve usar a API REST, a AWS Command Line Interface (AWS CLI) ou os AWS SDKs.
8. Na seção Outposts access point settings (Configurações do ponto de acesso do Outposts), insira o nome do ponto de acesso.

   Os pontos de acesso do S3 on Outposts simplificam o gerenciamento de acesso a dados em escala para conjuntos de dados compartilhados no S3 on Outposts. Os pontos de acesso são endpoints de rede nomeados que são anexados a buckets do Outposts que você pode usar para executar operações de objeto S3. Para obter mais informações, consulte Pontos de acesso.

   Os nomes de pontos de acesso devem ser exclusivos dentro da conta para essa região e Outpost, além de cumprir com as limitações e restrições do ponto de acesso.
9. Escolha a VPC para este ponto de acesso do Amazon S3 no Outposts.

   Se você não tiver uma VPC, escolha Create VPC (Criar VPC). Consulte mais informações em Criar pontos de acesso restritos a uma nuvem privada virtual no Guia do usuário do Amazon S3.

A Virtual Private Cloud (VPC) permite iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

10. (Opcional para uma VPC existente) Escolha uma Sub-rede de endpoint para o endpoint.

    Uma sub-rede é uma gama de endereços IP na VPC. Se você não tiver a sub-rede desejada, escolha Create subnet (Criar sub-rede). Para obter mais informações, consulte Redes para S3 on Outposts.

11. (Opcional para uma VPC existente) Escolha um Grupo de segurança de endpoint para o endpoint.

    Um grupo de segurança atua como um firewall virtual para controlar o tráfego de entrada e saída.

12. (Opcional para uma VPC existente) Escolha o Tipo de acesso ao endpoint:

    - Private (Privado): a ser usado com a VPC.
    - Customer owned IP (IP de propriedade do cliente): a ser usado com um grupo de endereços IP (grupo CoIP) de propriedade do cliente em sua rede on-premises.

13. (Opcional) Especifique a política de ponto de acesso do Outpost. O console exibe automaticamente o nome do recurso da Amazon (ARN) do ponto de acesso, que você pode usar na política.
14. Escolha Create Outposts bucket (Criar bucket do Outposts).

> **Note**
>
> Pode levar até cinco minutos para que seu endpoint do Outpost seja criado e seu bucket esteja pronto para uso. Para definir configurações de bucket adicionais, escolha View details (Visualizar detalhes).

Próximas etapas

Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode

usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Depois de criar um bucket no S3 on Outposts, um ponto de acesso e um endpoint, você pode usar a AWS CLI ou o SDK para Java para carregar um objeto no bucket. Para obter mais informações, consulte Fazer upload de um objeto em um bucket do S3 on Outposts.

Como começar a usar a AWS CLI e o SDK para Java

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (`OUTPOSTS`), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Para começar a usar o S3 on Outposts, você deve criar um bucket, um ponto de acesso e um endpoint. Depois, você pode carregar objetos no bucket. Os exemplos a seguir mostram como começar a usar o S3 on Outposts com a AWS CLI e o SDK para Java. Para começar a usar o console, consulte Conceitos básicos do uso do Console de gerenciamento da AWS.

Tópicos

- Etapa 1: Criar um bucket
- Etapa 2: Criar um ponto de acesso
- Etapa 3: Criar um endpoint
- Etapa 4: Fazer upload de um objeto em um bucket do S3 on Outposts

Etapa 1: Criar um bucket

Os exemplos de AWS CLI e SDK para Java a seguir mostram como criar um bucket do S3 on Outposts.

AWS CLI

Example

O exemplo a seguir cria um bucket do S3 on Outposts (`s3-outposts:CreateBucket`) usando a AWS CLI. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-bucket --bucket example-outposts-bucket --outpost-
id op-01ac5d28a6a232904
```

SDK for Java

Example

Para ver exemplos de como criar um bucket do S3 Outposts com o AWS SDK para Java, consulte CreateOutpostsBucket.java nos exemplos de código do AWS SDK for Java 2.x.

Etapa 2: Criar um ponto de acesso

Para acessar o bucket do Amazon S3 on Outposts, você deve criar e configurar um ponto de acesso. Esses exemplos mostram como criar um ponto de acesso usando a AWS CLI e o SDK para Java.

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como `GetObject` e `PutObject`. Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual.

AWS CLI

Example

O exemplo da AWS CLI a seguir cria um ponto de acesso para um bucket do Outposts. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-access-point --account-id 123456789012
 --name example-outposts-access-point --bucket "arn:aws:s3-
```

```
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket" --vpc-configuration VpcId=example-vpc-12345
```

SDK for Java

Example

Para ver exemplos de como criar um ponto de acesso para um bucket do S3 Outposts com o AWS SDK para Java, consulte CreateOutpostsAccessPoint.java nos exemplos de código do AWS SDK para Java 2.x.

Etapa 3: Criar um endpoint

Para rotear solicitações para um ponto de acesso do Amazon S3 on Outposts, você deve criar e configurar um endpoint do S3 on Outposts. Para criar um endpoint, você precisará de uma conexão ativa com seu link de serviço com sua região de origem do Outposts. Cada nuvem privada virtual (VPC) em seu Outpost pode ter um endpoint associado. Para obter mais informações sobre cotas de endpoints, consulte Requisitos de rede do S3 on Outposts. Você deve criar um endpoint para poder acessar seus buckets do Outposts e executar operações de objeto. Para obter mais informações, consulte Endpoints.

Esses exemplos mostram como criar um endpoint usando a AWS CLI e o SDK para Java. Para obter mais informações sobre as permissões necessárias para criar e gerenciar endpoints, consulte Permissões para os endpoints do S3 on Outposts.

AWS CLI

Example

O seguinte exemplo da AWS CLI cria um endpoint para um Outpost usando o tipo de acesso a recursos da VPC. A VPC é derivada da sub-rede. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1
```

O exemplo a seguir da AWS CLI cria um endpoint para um Outpost usando o tipo de acesso do grupo de endereços IP de propriedade do cliente (grupo do CoIP). Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1 --access-type CustomerOwnedIp --
customer-owned-ipv4-pool ipv4pool-coip-12345678901234567
```

SDK for Java

Example

Para ver exemplos de como criar um endpoint para um S3 Outpost com o AWS SDK para Java, consulte CreateOutpostsEndPoint.java nos exemplos de código do AWS SDK para Java 2.x.

Etapa 4: Fazer upload de um objeto em um bucket do S3 on Outposts

Para carregar um objeto, consulte Fazer upload de um objeto em um bucket do S3 on Outposts.

Redes para S3 on Outposts

Você pode usar o Amazon S3 on Outposts para armazenar e recuperar objetos on-premises para aplicações que exijam acesso a dados locais, processamento de dados e residência de dados. Esta seção descreve os requisitos de rede para acessar o S3 on Outposts.

Tópicos

- Escolher seu tipo de acesso às redes
- Acessar buckets e objetos do S3 on Outposts
- Interfaces de rede elástica entre contas

Escolher seu tipo de acesso às redes

É possível acessar o S3 on Outposts de dentro de uma VPC ou de sua rede on-premises. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint. Isso mantém o tráfego entre a VPC e os buckets do S3 on Outposts na rede da AWS. Ao criar um endpoint, é necessário especificar o tipo de acesso ele como `Private` (para roteamento de VPC) ou `CustomerOwnedIp` [para um grupo de endereços IP do cliente (CoIP)].

- `Private` (para roteamento de VPC): se você não especificar o tipo de acesso, o S3 on Outposts usará `Private` por padrão. Com o tipo de acesso `Private`, as instâncias em sua VPC não exigem que endereços IP públicos se comuniquem com recursos no Outpost. É possível trabalhar com o S3 on Outposts de dentro de uma VPC. Esse tipo de endpoint é acessível pela rede on-premises por meio do roteamento direto de VPC. Para obter mais informações, consulte Tabelas de rotas do gateway local no Guia do usuário do AWS Outposts.
- `CustomerOwnedIp` (para grupo de CoIP): se você não usar o padrão para o tipo de acesso `Private` e escolher `CustomerOwnedIp`, especifique um intervalo de endereços IP. Você pode usar esse tipo de acesso para trabalhar com o S3 on Outposts de sua rede on-premises e em uma VPC. Ao acessar o S3 on Outposts em uma VPC, seu tráfego é limitado à largura de banda do gateway local.

Acessar buckets e objetos do S3 on Outposts

Para acessar buckets e objetos do S3 on Outposts, é preciso ter o seguinte:

- Um ponto de acesso para a VPC.
- Um endpoint para a mesma VPC.
- Uma conexão ativa entre seu Outpost e sua Região da AWS. Para obter mais informações sobre como conectar seu Outpost a uma região, consulte Conectividade do Outpost para regiões da AWS no Guia do usuário do AWS Outposts.

Para obter mais informações sobre como acessar buckets e objetos no S3 on Outposts, consulte Trabalhar com buckets do S3 on Outposts e Trabalhar com objetos usando o S3 on Outposts.

Interfaces de rede elástica entre contas

Os endpoints do S3 on Outposts são recursos que recebem nomes de recurso da Amazon (ARNs). Quando esses endpoints são criados, o AWS Outposts configura múltiplas interfaces de rede elástica entre contas. As interfaces de rede elástica entre contas do S3 on Outposts são semelhantes a outras interfaces de rede, com uma exceção: o S3 on Outposts associa as interfaces de rede elástica entre contas a instâncias do Amazon EC2.

O Sistema de Nomes de Domínio (DNS) do S3 on Outposts balanceia a carga de suas solicitações na interface de rede elástica entre contas. O S3 on Outposts cria a interface de rede elástica entre contas em sua conta da AWS que é visível no painel Network interfaces (Interfaces de rede) do console do Amazon EC2.

Para endpoints que usam o tipo de acesso ao grupo de CoIP, o S3 on Outposts aloca e associa endereços IP à interface de rede elástica entre contas do grupo de CoIP configurado.

Trabalhar com buckets do S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos on-premises para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (`OUTPOSTS`), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que no Amazon S3, incluindo políticas de acesso, criptografia e marcação. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Você se comunica com os buckets do Outpost usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). Para acessar buckets e objetos do S3 on Outposts, é preciso ter um ponto de acesso para a VPC e um endpoint para a mesma VPC. Para obter mais informações, consulte Redes para S3 on Outposts.

Buckets

No S3 on Outposts, os nomes de bucket são exclusivos de um Outpost e exigem o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do bucket para identificá-los.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/bucket-name
```

Para obter mais informações, consulte ARNs de recurso para S3 no Outposts.

Pontos de acesso

O Amazon S3 on Outposts oferece suporte a pontos de acesso somente de nuvem privada virtual (VPC) como o único meio de acessar os buckets do Outposts.

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como `GetObject` e `PutObject`. Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 on Outposts. O ARN do ponto de acesso inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Endpoints

Para rotear solicitações para um ponto de acesso do S3 no Outposts, você deve criar e configurar um endpoint do S3 no Outposts. Com endpoints do S3 on Outposts, você pode conectar sua VPC de forma privada ao bucket do Outposts. Os endpoints do S3 on Outposts são identificadores de recursos uniformes (URIs) virtuais do ponto de entrada para o bucket do S3 on Outposts. Eles são componentes de VPC escalados horizontalmente, redundantes e altamente disponíveis.

Cada nuvem privda virtual (VPC) em seu Outpost pode ter um endpoint associado, e você pode ter até 100 endpoints por Outpost. Você deve criar esses endpoints para poder acessar seus buckets do Outposts e executar operações de objeto. Criar esses endpoints também possibilita que o modelo e os comportamentos da API sejam os mesmos ao permitir que as mesmas operações funcionem no S3 e no S3 on Outposts.

Operações de API no S3 on Outposts

Para gerenciar operações de API no bucket do Outposts, o S3 on Outposts hospeda um endpoint separado que é distinto do endpoint do Amazon S3. Este endpoint é `s3-outposts.region.amazonaws.com`.

Para usar as operações de API do Amazon S3, é necessário assinar o bucket e os objetos usando o formato de ARN correto. Você deve passar ARNs para operações de API para que o Amazon S3 possa determinar se a solicitação é para o Amazon S3 (`s3-control.region.amazonaws.com`) ou para o S3 on Outposts (`s3-outposts.region.amazonaws.com`). Com base no formato ARN, o S3 pode então assinar e rotear a solicitação adequadamente.

Sempre que uma solicitação é enviada para o plano de controle do Amazon S3, o SDK extrai os componentes do ARN e inclui o cabeçalho adicional `x-amz-outpost-id` com o valor `outpost-id` extraído do ARN. O nome do serviço do ARN é usado para assinar a solicitação antes de ser roteada para o endpoint do S3 on Outposts. Esse comportamento se aplica a todas as operações de API manipuladas pelo cliente `s3control`.

A tabela a seguir lista as operações de API estendidas para o Amazon S3 on Outposts e suas alterações em relação ao Amazon S3.

solicitações de	Valor do parâmetro do S3 no Outposts	
`CreateBucket`	Nome do bucket como ARN, ID do Outpost	
`ListRegionalBuckets`	ID do Outpost	
`DeleteBucket`	Nome do bucket como ARN	
`DeleteBucketLifecycleConfiguration`	Nome do bucket como ARN	
`GetBucketLifecycleConfiguration`	Nome do bucket como ARN	
`PutBucketLifecycleConfiguration`	Nome do bucket como ARN	
`GetBucketPolicy`	Nome do bucket como ARN	
`PutBucketPolicy`	Nome do bucket como ARN	
`DeleteBucketPolicy`	Nome do bucket como ARN	
`GetBucketTagging`	Nome do bucket como ARN	
`PutBucketTagging`	Nome do bucket como ARN	
`DeleteBucketTagging`	Nome do bucket como ARN	
`CreateAccessPoint`	Nome do ponto de acesso como ARN	
`DeleteAccessPoint`	Nome do ponto de acesso como ARN	

solicitações de	Valor do parâmetro do S3 no Outposts	
`GetAccessPoint`	Nome do ponto de acesso como ARN	
`GetAccessPoint`	Nome do ponto de acesso como ARN	
`ListAccessPoints`	Nome do ponto de acesso como ARN	
`PutAccessPointPolicy`	Nome do ponto de acesso como ARN	
`GetAccessPointPolicy`	Nome do ponto de acesso como ARN	
`DeleteAccessPointPolicy`	Nome do ponto de acesso como ARN	

Criar e gerenciar o bucket do S3 no Outposts

Para obter mais informações sobre como criar e gerenciar buckets do S3 on Outposts, consulte os tópicos a seguir.

Criar um bucket do S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (`OUTPOSTS`), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por

meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

> **Note**
>
> A Conta da AWS que cria o bucket é proprietária dele e é a única que pode confirmar suas ações. Os buckets têm propriedades de configuração como Outpost, etiquetas, criptografia padrão e configurações de ponto de acesso. As configurações de ponto de acesso incluem a nuvem privada virtual (VPC), a política do ponto de acesso para acessar os objetos no bucket e outros metadados. Para ter mais informações, consulte Especificações do Amazon S3 no Outposts.
>
> Se você quiser criar um bucket que use o AWS PrivateLink para fornecer acesso ao gerenciamento de buckets e endpoints por meio de endpoints da VPC de interface na nuvem privada virtual (VPC), consulte AWS PrivateLink para S3 no Outposts.

Os exemplos a seguir mostram como criar um bucket do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha Create Outposts bucket (Criar bucket do Outposts).
4. Em Bucket name (Nome do bucket), insira um nome compatível com o Sistema de Nome de Domínio (DNS) para seu bucket.

   O nome do bucket deve:

   - Ser único dentro da Conta da AWS, do Outpost e da Região da AWS na qual o Outpost está alojado.
   - Ter entre 3 e 63 caracteres.
   - Não contém caracteres maiúsculos.
   - Começar com uma letra minúscula ou um número.

Depois de criado o bucket, você não pode mudar seu nome. Consulte informações sobre como nomear buckets em Regras de nomenclatura de buckets de diretório no Guia do usuário do Amazon S3.

> **Important**
>
> Evite incluir informações confidenciais, como números de conta, no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

5. Em Outpost, escolha o Outpost onde você quer que o bucket resida.
6. Em Bucket Versioning (Versionamento de bucket), defina o estado de versionamento do S3 para seu bucket do S3 no Outposts como uma das seguintes opções:

   - Disable (Desabilitar) (padrão): o bucket permanece sem versão.
   - Enable (Habilitar): habilita o versionamento do S3 para os objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo.

   Para obter mais informações sobre o S3 Versioning, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.
7. (Opcional) Adicione as optional tags (etiquetas opcionais) que você gostaria de associar ao bucket do Outposts. Você pode usar etiquetas para monitorar os critérios para projetos específicos ou grupos de projetos ou para rotular seus buckets usando etiquetas de alocação de custo.

   Por padrão, todos os objetos armazenados no bucket do Outposts são armazenados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Você também pode optar explicitamente por armazenar objetos usando a criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C). Para alterar o tipo de criptografia, você deve usar a API REST, a AWS Command Line Interface (AWS CLI) ou os AWS SDKs.
8. Na seção Outposts access point settings (Configurações do ponto de acesso do Outposts), insira o nome do ponto de acesso.

   Os pontos de acesso do S3 on Outposts simplificam o gerenciamento de acesso a dados em escala para conjuntos de dados compartilhados no S3 on Outposts. Os pontos de acesso são

endpoints de rede nomeados que são anexados a buckets do Outposts que você pode usar para executar operações de objeto S3. Para ter mais informações, consulte Pontos de acesso.

Os nomes de pontos de acesso devem ser exclusivos dentro da conta para essa região e Outpost, além de cumprir com as limitações e restrições do ponto de acesso.

9. Escolha a VPC para este ponto de acesso do Amazon S3 no Outposts.

   Se você não tiver uma VPC, escolha Create VPC (Criar VPC). Consulte mais informações em Criar pontos de acesso restritos a uma nuvem privada virtual no Guia do usuário do Amazon S3.

   A Virtual Private Cloud (VPC) permite iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

10. (Opcional para uma VPC existente) Escolha uma Sub-rede de endpoint para o endpoint.

    Uma sub-rede é uma gama de endereços IP na VPC. Se você não tiver a sub-rede desejada, escolha Create subnet (Criar sub-rede). Para obter mais informações, consulte Redes para S3 on Outposts.

11. (Opcional para uma VPC existente) Escolha um Grupo de segurança de endpoint para o endpoint.

    Um grupo de segurança atua como um firewall virtual para controlar o tráfego de entrada e saída.

12. (Opcional para uma VPC existente) Escolha o Tipo de acesso ao endpoint:

    - Private (Privado): a ser usado com a VPC.
    - Customer owned IP (IP de propriedade do cliente): a ser usado com um grupo de endereços IP (grupo CoIP) de propriedade do cliente em sua rede on-premises.

13. (Opcional) Especifique a política de ponto de acesso do Outpost. O console exibe automaticamente o nome do recurso da Amazon (ARN) do ponto de acesso, que você pode usar na política.

14. Escolha Create Outposts bucket (Criar bucket do Outposts).

> **Note**
>
> Pode levar até cinco minutos para que seu endpoint do Outpost seja criado e seu bucket esteja pronto para uso. Para definir configurações de bucket adicionais, escolha View details (Visualizar detalhes).

Como usar a AWS CLI

Example

O exemplo a seguir cria um bucket do S3 on Outposts (`s3-outposts:CreateBucket`) usando a AWS CLI. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-bucket --bucket example-outposts-bucket --outpost-
id op-01ac5d28a6a232904
```

Usar o AWS SDK para Java

Example

Para ver exemplos de como criar um bucket do S3 Outposts com o AWS SDK para Java, consulte CreateOutpostsBucket.java nos exemplos de código do AWS SDK for Java 2.x.

Adicionar etiquetas aos buckets do S3 on Outposts

Você pode adicionar etiquetas para seus buckets do Amazon S3 on Outpost para monitorar o custo de armazenamento e outros critérios para projetos individuais ou grupos de projetos.

> **Note**
>
> A Conta da AWS que cria o bucket é proprietária dele e é a única que pode alterar suas tags.

Uso do console do S3

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts com as etiquetas que você deseja editar.
4. Escolha a guia Properties (Propriedades).
5. Em Tags, escolha Edit (Editar).
6. Escolha Add new tag (Adicionar nova etiqueta) e insira a Key (Chave) e um Value (Valor) opcional.

   Adicione todas as etiquetas que você gostaria de associar ao bucket do Outposts para monitorar outros critérios referentes a projetos individuais ou grupos de projetos.
7. Selecione Save changes.

Uso do AWS CLI

O exemplo de AWS CLI a seguir aplica uma configuração de marcação a um bucket do S3 on Outposts usando um documento JSON na pasta atual que especifica as etiquetas (*tagging.json*). Para usar esse exemplo, substitua cada *user input placeholder* por suas próprias informações.

```
aws s3control put-bucket-tagging --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --tagging file://tagging.json

tagging.json

{
   "TagSet": [
     {
       "Key": "organization",
       "Value": "marketing"
     }
   ]
}
```

O exemplo de AWS CLI a seguir aplica uma configuração de marcação a um bucket do S3 on Outposts diretamente da linha de comando.

```
aws s3control put-bucket-tagging --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --tagging 'TagSet=[{Key=organization,Value=marketing}]'
```

Para obter mais informações sobre esse comando, consulte put-bucket-tagging na Referência da AWS CLI.

Gerenciar o acesso a um bucket do Amazon S3 on Outposts usando uma política de bucket

Uma política de bucket é baseada em recursos do AWS Identity and Access Management (IAM) que você pode usar para conceder permissões de acesso ao bucket e aos objetos nele contidos. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. As políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Política de bucket.

Você pode atualizar sua política de bucket para gerenciar o acesso ao bucket do Amazon S3 on Outposts. Para obter mais informações, consulte os tópicos a seguir.

Tópicos

- Adicionar ou editar uma política para um bucket do Amazon S3 on Outposts
- Visualizar a política do bucket do Amazon S3 on Outposts
- Excluir a política do bucket do Amazon S3 on Outposts
- Exemplos de políticas de bucket

Adicionar ou editar uma política para um bucket do Amazon S3 on Outposts

Uma política de bucket é baseada em recursos do AWS Identity and Access Management (IAM) que você pode usar para conceder permissões de acesso ao bucket e aos objetos nele contidos. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. As políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Política de bucket.

Os tópicos a seguir mostram como atualizar sua política de bucket do Amazon S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) ou o AWS SDK para Java.

Usar o console do S3

Para criar ou editar uma política de bucket

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts cuja política de bucket você deseja editar.
4. Escolha a aba Permissões.
5. Na seção Outposts bucket policy (Política de bucket do Outposts), para criar ou editar uma nova política, escolha Edit (Editar).

   Agora, você pode adicionar ou editar a política de bucket do S3 on Outposts. Para obter mais informações, consulte Configurar o IAM com o S3 on Outposts.

Usar a AWS CLI

O exemplo da AWS CLI a seguir coloca uma política em um bucket do Outposts.

1. Salve a política de bucket a seguir em um arquivo JSON. Neste exemplo, o nome do arquivo é `policy1.json`. Substitua os *`user input placeholders`* por suas próprias informações.

   JSON

```
{
   "Version":"2012-10-17",
   "Id":"testBucketPolicy",
   "Statement":[
      {
         "Sid":"st1",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":[
            "s3-outposts:GetObject",
            "s3-outposts:PutObject",
            "s3-outposts:DeleteObject",
            "s3-outposts:ListBucket"
```

```
        ],
        "Resource":"arn:aws:s3-outposts:us-
east-1:123456789012:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket"
      }
   ]
}
```

2. Envie o arquivo JSON como parte do comando `put-bucket-policy` da CLI. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control put-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --policy file://policy1.json
```

Usar o AWS SDK para Java

O exemplo do SDK for Java a seguir coloca uma política em um bucket do Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void putBucketPolicy(String bucketArn) {

    String policy = "{\"Version\":\"2012-10-17\",\"Id\":\"testBucketPolicy\",
\"Statement\":[{\"Sid\":\"st1\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"" +
 AccountId+ "\"},\"Action\":\"s3-outposts:*\",\"Resource\":\"" + bucketArn + "\"}]}";

    PutBucketPolicyRequest reqPutBucketPolicy = new PutBucketPolicyRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn)
            .withPolicy(policy);

    PutBucketPolicyResult respPutBucketPolicy =
 s3ControlClient.putBucketPolicy(reqPutBucketPolicy);
    System.out.printf("PutBucketPolicy Response: %s%n",
 respPutBucketPolicy.toString());

}
```

Visualizar a política do bucket do Amazon S3 on Outposts

Uma política de bucket é baseada em recursos do AWS Identity and Access Management (IAM) que você pode usar para conceder permissões de acesso ao bucket e aos objetos nele contidos. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. As políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Política de bucket.

Os tópicos a seguir mostram como visualizar sua política de bucket do Amazon S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) ou o AWS SDK para Java.

Uso do console do S3

Para criar ou editar uma política de bucket

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts cuja permissão você deseja editar.
4. Escolha a guia Permissions.
5. Na seção Outposts bucket policy (Política de bucket do Outposts), você pode revisar sua política de bucket existente. Para obter mais informações, consulte Configurar o IAM com o S3 on Outposts.

Usar a AWS CLI

O exemplo da AWS CLI a seguir obtém uma política para um bucket do Outposts. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket
```

Usar o AWS SDK para Java

O exemplo do SDK for Java a seguir obtém uma política para um bucket do Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void getBucketPolicy(String bucketArn) {

    GetBucketPolicyRequest reqGetBucketPolicy = new GetBucketPolicyRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn);

    GetBucketPolicyResult respGetBucketPolicy =
 s3ControlClient.getBucketPolicy(reqGetBucketPolicy);
    System.out.printf("GetBucketPolicy Response: %s%n",
 respGetBucketPolicy.toString());

}
```

Excluir a política do bucket do Amazon S3 on Outposts

Uma política de bucket é baseada em recursos do AWS Identity and Access Management (IAM) que você pode usar para conceder permissões de acesso ao bucket e aos objetos nele contidos. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. As políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Política de bucket.

Os tópicos a seguir mostram como visualizar sua política de bucket do Amazon S3 on Outposts usando o Console de gerenciamento da AWS ou a AWS Command Line Interface (AWS CLI).

Uso do console do S3

Para excluir uma política de bucket

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts cuja permissão você deseja editar.
4. Escolha a guia Permissions.
5. Na seção Outposts bucket policy (Política de bucket do Outposts), escolha Delete (Excluir).
6. Confirme a exclusão.

Uso do AWS CLI

O exemplo a seguir exclui a política de um bucket do S3 on Outposts (`s3-outposts:DeleteBucket`) usando a AWS CLI. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control delete-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket
```

Exemplos de políticas de bucket

Com as políticas de bucket do S3 no Outposts, você pode proteger o acesso a objetos em seus buckets do S3 no Outposts, para que somente usuários com as permissões apropriadas possam acessá-los. Você pode até mesmo impedir que usuários autenticados sem as permissões apropriadas acessem seus recursos do S3 no Outposts.

Esta seção apresenta exemplos de casos de uso típicos de políticas de bucket do S3 no Outposts. Para testar essas políticas, substitua *`user input placeholders`* por suas informações (como o nome do seu bucket).

Para conceder ou negar permissões para um conjunto de objetos, você pode usar caracteres curinga (*) em nomes de recursos da Amazon (ARNs) e outros valores. Por exemplo, você pode controlar o acesso a grupos de objetos que começam com um prefixo ou termine com uma determinada extensão, como `.html`.

Para obter mais informações sobre a linguagem da política do AWS Identity and Access Management (IAM), consulte Configurar o IAM com o S3 on Outposts.

> **Note**
>
> Ao testar as permissões s3outposts usando o console do Amazon S3, você deve conceder permissões adicionais exigidas pelo console, como `s3outposts:createendpoint`, `s3outposts:listendpoints` e assim por diante.

Recursos adicionais para criar políticas de bucket

- Para conferir uma lista de ações, recursos e chaves de condição de políticas do IAM que você pode usar ao criar uma política de bucket do S3 no Outposts, consulte Actions, resources, and condition keys for Amazon S3 on Outposts.
- Para obter orientação sobre como criar uma política do S3 no Outposts, consulte Adicionar ou editar uma política para um bucket do Amazon S3 on Outposts.

Tópicos

- Gerenciar o acesso a um bucket do Amazon S3 no Outposts com base em endereços IP específicos

Gerenciar o acesso a um bucket do Amazon S3 no Outposts com base em endereços IP específicos

Uma política de bucket é baseada em recursos do AWS Identity and Access Management (IAM) que você pode usar para conceder permissões de acesso ao bucket e aos objetos nele contidos. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. As políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Política de bucket.

Restringir o acesso a endereços IP específicos

O exemplo a seguir impede que todos os usuários executem operações do S3 no Outposts em objetos nos buckets especificados, a menos que a solicitação tenha origem no intervalo de endereços IP especificado.

> **Note**
>
> Ao restringir o acesso a um endereço IP específico, especifique quais endpoints da VPC, endereços IP de origem da VPC ou endereços IP externos podem acessar o bucket do S3 no Outposts. Caso contrário, você poderá perder o acesso ao bucket se a sua política negar aos usuários a execução de qualquer operação s3outposts em objetos no bucket do S3 no Outposts sem as permissões adequadas já em vigor.

A instrução `Condition` dessa política identifica *`192.0.2.0/24`* como o intervalo de endereços IP versão 4 (IPv4) permitidos.

O bloco `Condition` usa a condição `NotIpAddress` e a chave de condição `aws:SourceIp`, que é uma chave de condição que abrange toda a AWS. A chave de condição `aws:SourceIp` só pode ser usada para intervalos de endereços IP públicos. Para obter mais informações sobre essas chaves de condição, consulte Actions, resources, and condition keys for S3 on Outposts. Os valores IPv4 `aws:SourceIp` usam a notação CIDR padrão. Para obter mais informações, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

> **Warning**
>
> Antes de usar essa política do S3 no Outposts, substitua o intervalo de endereços IP *`192.0.2.0/24`* desse exemplo por um valor apropriado para o seu caso de uso. Caso contrário, você perderá a capacidade de acessar o bucket.

```
{
    "Version": "2012-10-17",
    "Id": "S3OutpostsPolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3-outposts:*",
            "Resource": [
                "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
accesspoint/EXAMPLE-ACCESS-POINT-NAME",
                "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/amzn-s3-demo-bucket"
            ],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                }
            }
        }
    ]
}
```

Permitir endereços IPv4 e IPv6

Ao começar a usar os endereços IPv6, recomendamos que você atualize todas as políticas da sua organização com os intervalos de endereços IPv6 além dos intervalos de IPv4 existentes. Isso ajudará a garantir que as políticas continuem funcionando à medida que você faz a transição para IPv6.

O exemplo de política de bucket do S3 no Outposts a seguir mostra como misturar intervalos de endereços IPv4 e IPv6 para cobrir todos os endereços IP válidos de sua organização. A política de exemplo permite acesso aos endereços IP *192.0.2.1* e *2001:DB8:1234:5678::1* e nega acesso aos endereços *203.0.113.1* e *2001:DB8:1234:5678:ABCD::1*.

A chave de condição `aws:SourceIp` só pode ser usada para intervalos de endereços IP públicos. Os valores de IPv6 para `aws:SourceIp` devem estar em formato CIDR padrão. Para IPv6, oferecemos suporte ao uso de `::` para representar um intervalo de IPv6 (por exemplo `2001:DB8:1234:5678::/64`). Para obter mais informações, consulte Operadores de condição de endereço IP no Guia do usuário do IAM.

> **Warning**
>
> Substitua os intervalos de endereços IP neste exemplo por valores apropriados para o seu caso de uso antes de usar esta política do S3 no Outposts. Caso contrário, você pode perder a capacidade de acessar seu bucket.

JSON

```
{
    "Id": "S3OutpostsPolicyId2",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowIPmix",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "s3-outposts:GetObject",
```

```
                "s3-outposts:PutObject",
                "s3-outposts:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket",
                "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "2001:DB8:1234:5678::/64"
                    ]
                },
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "203.0.113.0/24",
                        "2001:DB8:1234:5678:ABCD::/80"
                    ]
                }
            }
        }
    ]
}
```

Listar buckets do Amazon S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (0UTP0STS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Para obter mais informações sobre como trabalhar com buckets no S3 on Outposts, consulte Trabalhar com buckets do S3 on Outposts.

Os exemplos a seguir mostram como retornar uma lista dos buckets do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS CLI e o AWS SDK para Java.

Usar o console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Em Outposts buckets (Buckets do Outposts), revise sua lista de buckets do S3 on Outposts.

Como usar o AWS CLI

O exemplo da AWS CLI a seguir obtém uma lista de buckets em um Outpost. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte list-regional-buckets na Referência da AWS CLI.

```
aws s3control list-regional-buckets --account-id 123456789012 --outpost-
id op-01ac5d28a6a232904
```

Usar o AWS SDK para Java

O exemplo do SDK para Java a seguir obtém uma lista de buckets em um Outpost. Para obter mais informações, consulte ListRegionalBuckets na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void listRegionalBuckets() {

    ListRegionalBucketsRequest reqListBuckets = new ListRegionalBucketsRequest()
            .withAccountId(AccountId)
            .withOutpostId(OutpostId);

    ListRegionalBucketsResult respListBuckets =
 s3ControlClient.listRegionalBuckets(reqListBuckets);
    System.out.printf("ListRegionalBuckets Response: %s%n",
 respListBuckets.toString());
```

```
}
```

Obter um bucket do S3 on Outposts usando a AWS CLI e o SDK para Java

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (0UTP0STS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Os exemplos a seguir mostram como obter um bucket do S3 on Outposts usando a AWS CLI e o AWS SDK para Java.

> **Note**
>
> Ao trabalhar com o Amazon S3 on Outposts por meio da AWS CLI ou de AWSSDKs, forneça o ARN do ponto de acesso do Outpost no lugar do nome do bucket. O ARN do ponto de acesso assume a forma a seguir, em que *region* é o código da Região da AWS em que se encontra o Outpost:
> `arn:aws:s3-outposts:`*region*`:`*123456789012*`:outpost/`*op-01ac5d28a6a232904*`/accesspoint/`*example-outposts-access-point*
> Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

Como usar o AWS CLI

O exemplo do S3 on Outposts a seguir obtém um bucket usando a AWS CLI. Para usar esse comando, substitua cada *user input placeholder* por suas próprias informações. Para obter mais informações sobre esse comando, consulte get-bucket na Referência da AWS CLI.

```
aws s3control get-bucket --account-id 123456789012 --bucket "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket"
```

Usar o AWS SDK para Java

O exemplo do S3 no Outposts a seguir obtém um bucket usando o SDK para Java. Para obter mais informações, consulte GetBucket na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void getBucket(String bucketArn) {

    GetBucketRequest reqGetBucket = new GetBucketRequest()
            .withBucket(bucketArn)
            .withAccountId(AccountId);

    GetBucketResult respGetBucket = s3ControlClient.getBucket(reqGetBucket);
    System.out.printf("GetBucket Response: %s%n", respGetBucket.toString());

}
```

Excluir seu bucket do S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (OUTPOSTS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Para obter mais informações sobre como trabalhar com buckets no S3 on Outposts, consulte Trabalhar com buckets do S3 on Outposts.

A Conta da AWS que cria o bucket é proprietária dele e é a única que pode excluí-lo.

> **Note**
>
> - Os buckets do Outposts devem estar vazios antes de serem excluídos.
>
> O console do Amazon S3 não é compatível com ações de objeto do S3 on Outposts. Para excluir objetos em um bucket do S3 on Outposts, você deve usar a API REST, a AWS CLI ou os AWS SDKs.
> - Antes de excluir um bucket do Outposts, você deve excluir os pontos de acesso do Outposts para o bucket. Para obter mais informações, consulte Excluir um ponto de acesso.
> - Você não pode recuperar um bucket depois que ele foi excluído.

Os exemplos a seguir mostram como excluir um bucket do S3 on Outposts usando o Console de gerenciamento da AWS e a AWS Command Line Interface (AWS CLI).

Uso do console do S3

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket que você deseja excluir e escolha Delete (Excluir).
4. Confirme a exclusão.

Uso do AWS CLI

O exemplo a seguir exclui um bucket do S3 on Outposts (`s3-outposts:DeleteBucket`) usando a AWS CLI. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control delete-bucket --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket
```

Trabalhar com pontos de acesso do Amazon S3 on Outposts

Para acessar o bucket do Amazon S3 on Outposts, você deve criar e configurar um ponto de acesso.

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como `GetObject` e `PutObject`. Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual.

> **Note**
>
> A Conta da AWS que cria o bucket do Outposts é proprietária dele e é a única que pode atribuir pontos de acesso a ele.

As seções a seguir descrevem como criar e gerenciar pontos de acesso para buckets do S3 on Outposts.

Tópicos

- Criar um ponto de acesso do S3 on Outposts
- Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts
- Exibir informações sobre uma configuração de ponto de acesso
- Visualizar uma lista dos pontos de acesso do Amazon S3 on Outposts
- Excluir um ponto de acesso
- Adicionar ou editar uma política de ponto de acesso
- Visualizar uma política para um ponto de acesso do S3 on Outposts

Criar um ponto de acesso do S3 on Outposts

Para acessar o bucket do Amazon S3 on Outposts, você deve criar e configurar um ponto de acesso.

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como

`GetObject` e `PutObject`. Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual.

Os exemplos a seguir mostram como criar um ponto de acesso do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

> **Note**
>
> A Conta da AWS que cria o bucket do Outposts é proprietária dele e é a única que pode atribuir pontos de acesso a ele.

Usar o console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts para o qual deseja criar um ponto de acesso do Outposts.
4. Escolha a aba Outposts access points (Pontos de acesso do Outposts).
5. Na seção Outposts access points (Pontos de acesso do Outposts), escolha Create Outposts access point (Criar ponto de acesso do Outposts).
6. Na seção Outposts access point settings (Configurações do ponto de acesso do Outposts), insira um nome para o ponto de acesso e escolha a nuvem privada virtual (VPC) dele.
7. Se você quiser adicionar uma política para o seu ponto de acesso, adicione-a na seção Outposts access point policy (Política de ponto de acesso do Outposts).

   Para obter mais informações, consulte Configurar o IAM com o S3 on Outposts.

Como usar a AWS CLI

Example

O exemplo da AWS CLI a seguir cria um ponto de acesso para um bucket do Outposts. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-access-point --account-id 123456789012
 --name example-outposts-access-point --bucket "arn:aws:s3-
```

```
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket" --vpc-configuration VpcId=example-vpc-12345
```

Usar o AWS SDK para Java

Example

Para ver exemplos de como criar um ponto de acesso para um bucket do S3 Outposts com o AWS SDK para Java, consulte CreateOutpostsAccessPoint.java nos exemplos de código do AWS SDK para Java 2.x.

Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts

Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Toda vez que você cria um ponto de acesso para um bucket, o S3 no Outposts gera automaticamente um alias de ponto de acesso. É possível usar esse alias de ponto de acesso em vez de um ARN de ponto de acesso para qualquer operação de plano de dados. Por exemplo, você pode usar um alias de ponto de acesso para realizar operações em nível de objeto, como PUT, GET, LIST e muito mais. Para obter uma lista dessas operações, consulte Operações de API do Amazon S3 para gerenciar objetos.

Os exemplos a seguir mostram um ARN e um alias de ponto de acesso para um ponto de acesso chamado *my-access-point*.

- ARN do ponto de acesso: `arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/my-access-point`
- Alias do ponto de acesso: *my-access-po*-*o01ac5d28a6a232904e8xz5w8ijx1qzlbp3i3kuse10*`--op-s3`

Para obter mais informações sobre ARNs, consulte Nomes de recurso da Amazon (ARNs) no Referência geral da AWS.

Para obter mais informações sobre alias de pontos de acesso, consulte os tópicos a seguir.

Tópicos

- Alias de pontos de acesso

- Usar um alias de ponto de acesso em uma operação de objeto do S3 no Outposts
- Limitações

Alias de pontos de acesso

Cria-se um alias de ponto de acesso dentro do mesmo namespace de um bucket do S3 no Outposts. Quando você cria um ponto de acesso, o S3 no Outposts gera automaticamente um alias de ponto de acesso que não poderá ser alterado. O alias de ponto de acesso atende a todos os requisitos de um nome de bucket válido do S3 no Outposts e consiste nas seguintes partes:

access point name prefix`-`*metadata*`--op-s3`

> **Note**
>
> O sufixo `--op-s3` é reservado para alias de pontos de acesso. Recomendamos que não o use para nomes de bucket ou ponto de acesso. Para obter mais informações sobre as regras para nomes de bucket do S3 no Outposts, consulte Trabalhar com buckets do S3 on Outposts.

Encontrar o alias do ponto de acesso

Os exemplos a seguir mostram como encontrar um ponto de acesso usando o console do Amazon S3 e a AWS CLI.

Example: Encontrar e copiar um alias de ponto de acesso no console do Amazon S3

Depois de criar um ponto de acesso no console, você pode obter o alias do ponto de acesso na coluna Access Point alias (Alias de ponto de acesso) na lista Access Points (Pontos de acesso).

Como copiar um alias de ponto de acesso

1. Abra o console do Amazon S3, em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Para copiar o alias do ponto de acesso, realize um dos seguintes procedimentos:
   - Na lista Access Points (Pontos de acesso), selecione o botão de opção ao lado do nome do ponto de acesso e escolha Copy Access Point alias (Copiar alias do ponto de acesso).

- Escolha o nome do ponto de acesso. Depois, em Outposts access point overview (Visão geral dos pontos de acesso do Outposts), copie o alias do ponto de acesso.

Example: Criar um ponto de acesso usando a AWS CLI e encontrar o alias do ponto de acesso na resposta

O exemplo daAWS CLI a seguir para o comando `create-access-point` cria o ponto de acesso e retorna o alias do ponto de acesso gerado automaticamente. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-access-point --bucket example-outposts-bucket --name example-
outposts-access-point --account-id 123456789012

{
    "AccessPointArn":
    "arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/
accesspoint/example-outposts-access-point",
    "Alias": "example-outp-o01ac5d28a6a232904e8xz5w8ijx1qzlbp3i3kuse10--op-s3"
}
```

Example: Obter um alias de ponto de acesso usando a AWS CLI

O exemplo a seguir da AWS CLI para o comando `get-access-point` retorna informações sobre o ponto de acesso especificado. Essas informações incluem o alias do ponto de acesso. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control get-access-point --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --name example-outposts-access-point --account-id 123456789012

{
    "Name": "example-outposts-access-point",
    "Bucket": "example-outposts-bucket",
    "NetworkOrigin": "Vpc",
    "VpcConfiguration": {
        "VpcId": "vpc-01234567890abcdef"
    },
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
```

```
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2022-09-18T17:49:15.584000+00:00",
    "Alias": "example-outp-o0b1d075431d83bebde8xz5w8ijx1qzlbp3i3kuse10--op-s3"
}
```

Example: Listar os pontos de acesso para encontrar um alias de ponto de acesso usando a AWS CLI

O exemplo a seguir da AWS CLI para o comando `list-access-points` lista informações sobre o ponto de acesso especificado. Essas informações incluem o alias do ponto de acesso. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control list-access-points --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket

{
    "AccessPointList": [
        {
            "Name": "example-outposts-access-point",
            "NetworkOrigin": "Vpc",
            "VpcConfiguration": {
                "VpcId": "vpc-01234567890abcdef"
            },
            "Bucket": "example-outposts-bucket",
            "AccessPointArn": "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point",
            "Alias": "example-outp-o0b1d075431d83bebde8xz5w8ijx1qzlbp3i3kuse10--op-s3"
        }
    ]
}
```

Usar um alias de ponto de acesso em uma operação de objeto do S3 no Outposts

Ao adotar pontos de acesso, é possível usar alias de pontos de acesso sem exigir alterações extensas de código.

Este exemplo da AWS CLI mostra uma operação `get-object` para um bucket S3 no Outposts. Este exemplo usa o alias do ponto de acesso como valor para `--bucket` em vez do ARN completo do ponto de acesso.

```
aws s3api get-object --bucket my-access-po-
o0b1d075431d83bebde8xz5w8ijx1qzlbp3i3kuse10--op-s3 --key  testkey  sample-object.rtf

{
    "AcceptRanges": "bytes",
    "LastModified": "2020-01-08T22:16:28+00:00",
    "ContentLength": 910,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
    "VersionId": "null",
    "ContentType": "text/rtf",
    "Metadata": {}
}
```

Limitações

- Os aliases não podem ser configurados por clientes.
- Não é possível excluir, modificar ou desabilitar aliases de um ponto de acesso.
- Não é possível usar um alias de ponto de acesso para operações do ambiente de gerenciamento do S3 no Outposts. Para obter uma lista das operações do ambiente de gerenciamento do S3 no Outposts, consulte Operações de API do Amazon S3 Control para gerenciar buckets.
- Não é possível usar alias em políticas do AWS Identity and Access Management (IAM).

Exibir informações sobre uma configuração de ponto de acesso

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como `GetObject` e `PutObject`. Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual.

Os tópicos a seguir mostram como retornar informações de configuração para um ponto de acesso do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Escolha o ponto de acesso do Outposts para o qual deseja exibir os detalhes da configuração.
4. Em Outposts access point overview (Visão geral do ponto de acesso do Outposts), examine os detalhes da configuração do ponto de acesso.

Como usar o AWS CLI

O exemplo da AWS CLI a seguir obtém um ponto de acesso para um bucket do Outposts. Substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control get-access-point --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

Usar o AWS SDK para Java

O exemplo do SDK for Java a seguir obtém um ponto de acesso para um bucket do Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void getAccessPoint(String accessPointArn) {

    GetAccessPointRequest reqGetAP = new GetAccessPointRequest()
            .withAccountId(AccountId)
            .withName(accessPointArn);

    GetAccessPointResult respGetAP = s3ControlClient.getAccessPoint(reqGetAP);
    System.out.printf("GetAccessPoint Response: %s%n", respGetAP.toString());

}
```

Visualizar uma lista dos pontos de acesso do Amazon S3 on Outposts

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como `GetObject` e `PutObject`. Com o S3 on Outposts, você deve usar pontos de acesso para acessar

qualquer objeto em um bucket do Outposts. Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual.

Os tópicos a seguir mostram como retornar uma lista de seus pontos de acesso do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Em Outposts access points (Pontos de acesso do Outposts), analise sua lista de pontos de acesso do S3 on Outposts.

Como usar o AWS CLI

O exemplo da AWS CLI a seguir lista os pontos de acesso de um bucket do Outposts. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control list-access-points --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket
```

Usar o AWS SDK para Java

O exemplo do SDK for Java a seguir lista os pontos de acesso para um bucket do Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void listAccessPoints(String bucketArn) {

    ListAccessPointsRequest reqListAPs = new ListAccessPointsRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn);

    ListAccessPointsResult respListAPs = s3ControlClient.listAccessPoints(reqListAPs);
    System.out.printf("ListAccessPoints Response: %s%n", respListAPs.toString());

}
```

Excluir um ponto de acesso

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como `GetObject` e `PutObject`. Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual.

Os exemplos a seguir mostram como excluir um ponto de acesso usando o Console de gerenciamento da AWS e a AWS Command Line Interface (AWS CLI).

Uso do console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Na seção Outposts access points (Pontos de acesso do Outposts), escolha o ponto de acesso do Outposts que deseja excluir.
4. Escolha Delete.
5. Confirme a exclusão.

Uso do AWS CLI

O exemplo da AWS CLI a seguir exclui um ponto de acesso do Outposts. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control delete-access-point --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

Adicionar ou editar uma política de ponto de acesso

Cada ponto de acesso tem permissões e controles de rede distintos que o Amazon S3 on Outposts aplica a qualquer solicitação feita por meio desse ponto de acesso. Cada ponto de acesso impõe uma política de ponto de acesso personalizada que funciona em conjunto com a política de bucket anexada ao bucket subjacente. Para obter mais informações, consulte Pontos de acesso.

Os tópicos a seguir mostram como adicionar ou editar a política de ponto de acesso do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts para o qual você deseja editar a política de ponto de acesso.
4. Escolha a aba Outposts access points (Pontos de acesso do Outposts).
5. Na seção Outposts access points (Pontos de acesso do Outposts), selecione o ponto de acesso cuja política você quer editar e escolha Edit policy (Editar política).
6. Adicione ou edite a política na seção da Outposts access point policy (Política do ponto de acesso do Outposts). Para obter mais informações, consulte Configurar o IAM com o S3 on Outposts.

Usar a AWS CLI

O exemplo da AWS CLI a seguir coloca uma política para um bucket do Outposts.

1. Salve a política de ponto de acesso a seguir em um arquivo JSON. Neste exemplo, o nome do arquivo é `appolicy1.json`. Substitua os *`user input placeholders`* por suas próprias informações.

```
{
   "Version":"2012-10-17",
   "Id":"exampleAccessPointPolicy",
   "Statement":[
      {
         "Sid":"st1",
         "Effect":"Allow",
         "Principal":{
            "AWS":"123456789012"
         },
         "Action":"s3-outposts:*",
         "Resource":"arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point
      }
```

```
    ]
}
```

2. Envie o arquivo JSON como parte do comando `put-access-point-policy` da CLI. Substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control put-access-point-policy --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --policy file://appolicy1.json
```

Usar o AWS SDK para Java

O exemplo do SDK for Java a seguir coloca uma política em um ponto de acesso do Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void putAccessPointPolicy(String accessPointArn) {

    String policy = "{\"Version\":\"2012-10-17\",\"Id\":\"testAccessPointPolicy\",
\"Statement\":[{\"Sid\":\"st1\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"" +
 AccountId + "\"},\"Action\":\"s3-outposts:*\",\"Resource\":\"" + accessPointArn +
 "\"}]}";

    PutAccessPointPolicyRequest reqPutAccessPointPolicy = new
 PutAccessPointPolicyRequest()
            .withAccountId(AccountId)
            .withName(accessPointArn)
            .withPolicy(policy);

    PutAccessPointPolicyResult respPutAccessPointPolicy =
 s3ControlClient.putAccessPointPolicy(reqPutAccessPointPolicy);
    System.out.printf("PutAccessPointPolicy Response: %s%n",
 respPutAccessPointPolicy.toString());
    printWriter.printf("PutAccessPointPolicy Response: %s%n",
 respPutAccessPointPolicy.toString());

}
```

Visualizar uma política para um ponto de acesso do S3 on Outposts

Cada ponto de acesso tem permissões e controles de rede distintos que o Amazon S3 on Outposts aplica a qualquer solicitação feita por meio desse ponto de acesso. Cada ponto de acesso impõe uma política de ponto de acesso personalizada que funciona em conjunto com a política de bucket anexada ao bucket subjacente. Para obter mais informações, consulte Pontos de acesso.

Para obter mais informações sobre como trabalhar com pontos de acesso no S3 on Outposts, consulte Trabalhar com buckets do S3 on Outposts.

Os tópicos a seguir mostram como visualizar ou editar a política de ponto de acesso do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Uso do console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Escolha o ponto de acesso do Outposts para o qual você deseja visualizar a política.
4. Na guia Permissions (Permissões), analise a política do ponto de acesso do S3 on Outposts.
5. Para editar uma política de ponto de acesso, consulte Adicionar ou editar uma política de ponto de acesso.

Uso do AWS CLI

O exemplo da AWS CLI a seguir obtém uma política para um ponto de acesso do Outposts. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-access-point-policy --account-id 123456789012 --name arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-access-point
```

Usar o AWS SDK para Java

O exemplo do SDK for Java a seguir obtém uma política para um ponto de acesso do Outposts.

```
import com.amazonaws.services.s3control.model.*;
```

```
public void getAccessPointPolicy(String accessPointArn) {

    GetAccessPointPolicyRequest reqGetAccessPointPolicy = new
 GetAccessPointPolicyRequest()
            .withAccountId(AccountId)
            .withName(accessPointArn);

    GetAccessPointPolicyResult respGetAccessPointPolicy =
 s3ControlClient.getAccessPointPolicy(reqGetAccessPointPolicy);
    System.out.printf("GetAccessPointPolicy Response: %s%n",
 respGetAccessPointPolicy.toString());
    printWriter.printf("GetAccessPointPolicy Response: %s%n",
 respGetAccessPointPolicy.toString());

}
```

Trabalhar com endpoints do Amazon S3 on Outposts

Para rotear solicitações para um ponto de acesso do Amazon S3 on Outposts, você deve criar e configurar um endpoint do S3 on Outposts. Para criar um endpoint, você precisará de uma conexão ativa com seu link de serviço com sua região de origem do Outposts. Cada nuvem privada virtual (VPC) em seu Outpost pode ter um endpoint associado. Para obter mais informações sobre cotas de endpoints, consulte Requisitos de rede do S3 on Outposts. Você deve criar um endpoint para poder acessar seus buckets do Outposts e executar operações de objeto. Para ter mais informações, consulte Endpoints.

Depois de criar um endpoint, você pode usar o campo “Status” para entender o estado do endpoint. Se seu Outposts estiver offline, ele retornará um CREATE_FAILED. Você pode conferir sua conexão de link de serviço, excluir o endpoint e repetir a operação de criação depois que sua conexão for retomada. Para ter uma lista de códigos de erro adicionais, veja abaixo. Para ter mais informações, consulte Endpoints.

API	Status	Código de erro do motivo da falha	Mensagem: motivo da falha
`CreateEndpoint`	Create_Failed	OutpostNotReachable	O endpoint não pôde ser criado porque a conexão do link de serviço com sua região de origem do Outposts está

API	Status	Código de erro do motivo da falha	Mensagem: motivo da falha
			inativa. Confira sua conexão, exclua o endpoint e tente novamente.
`CreateEndpoint`	Create_Failed	InternalError	O endpoint não pôde ser criado devido a um erro interno. Exclua o endpoint e crie novamente.
`DeleteEndpoint`	Delete_Failed	OutpostNotReachable	O endpoint não pôde ser excluído porque a conexão do link de serviço com sua região de origem do Outposts está inativa. Confira sua conexão e tente novamente.
`DeleteEndpoint`	Delete_Failed	InternalError	O endpoint não pôde ser excluído devido a um erro interno. Tente novamente.

Para obter mais informações sobre como trabalhar com buckets no S3 on Outposts, consulte Trabalhar com buckets do S3 on Outposts.

As seções a seguir descrevem como criar e gerenciar endpoints para o S3 on Outposts.

Tópicos

- Criar um endpoint em um Outpost
- Visualizar uma lista de endpoints do Amazon S3 on Outposts
- Excluir um endpoint do Amazon S3 on Outposts

Criar um endpoint em um Outpost

Para rotear solicitações para um ponto de acesso do Amazon S3 on Outposts, você deve criar e configurar um endpoint do S3 on Outposts. Para criar um endpoint, você precisará de uma conexão ativa com seu link de serviço com sua região de origem do Outposts. Cada nuvem privada virtual (VPC) em seu Outpost pode ter um endpoint associado. Para obter mais informações sobre cotas de endpoints, consulte Requisitos de rede do S3 on Outposts. Você deve criar um endpoint para

poder acessar seus buckets do Outposts e executar operações de objeto. Para ter mais informações, consulte Endpoints.

Permissões

Para obter mais informações sobre as permissões necessárias para criar um endpoint, consulte Permissões para os endpoints do S3 on Outposts.

Ao criar um endpoint, o S3 no Outposts também cria um perfil vinculado a serviço na Conta da AWS. Para ter mais informações, consulte Usar perfis vinculados a serviço para o Amazon S3 no Outposts.

Os exemplos a seguir mostram como criar um endpoint do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Escolha a guia Outposts endpoints (Endpoints do Outposts).
4. Escolha Create Outposts endpoint (Criar endpoint do Outposts).
5. Em Outpost, escolha o Outpost no qual o endpoint será criado.
6. Em VPC, escolha uma VPC que ainda não tenha um endpoint e que esteja em conformidade com as regras para endpoints do Outposts.

   A Virtual Private Cloud (VPC) permite iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

   Se você não tiver uma VPC, escolha Create VPC (Criar VPC). Consulte mais informações em Criar pontos de acesso restritos a uma nuvem privada virtual no Guia do usuário do Amazon S3.
7. Escolha Create Outposts endpoint (Criar endpoint do Outposts).

Como usar a AWS CLI

Example

O seguinte exemplo da AWS CLI cria um endpoint para um Outpost usando o tipo de acesso a recursos da VPC. A VPC é derivada da sub-rede. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1
```

O exemplo a seguir da AWS CLI cria um endpoint para um Outpost usando o tipo de acesso do grupo de endereços IP de propriedade do cliente (grupo do CoIP). Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1 --access-type CustomerOwnedIp --
customer-owned-ipv4-pool ipv4pool-coip-12345678901234567
```

Usar o AWS SDK para Java

Example

Para ver exemplos de como criar um endpoint para um S3 Outpost com o AWS SDK para Java, consulte CreateOutpostsEndPoint.java nos exemplos de código do AWS SDK para Java 2.x.

Visualizar uma lista de endpoints do Amazon S3 on Outposts

Para rotear solicitações para um ponto de acesso do Amazon S3 on Outposts, você deve criar e configurar um endpoint do S3 on Outposts. Para criar um endpoint, você precisará de uma conexão ativa com seu link de serviço com sua região de origem do Outposts. Cada nuvem privada virtual (VPC) em seu Outpost pode ter um endpoint associado. Para obter mais informações sobre cotas de endpoints, consulte Requisitos de rede do S3 on Outposts. Você deve criar um endpoint para poder acessar seus buckets do Outposts e executar operações de objeto. Para obter mais informações, consulte Endpoints.

Os exemplos a seguir mostram como retornar uma lista de seus endpoints do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Na página Outposts access points (Pontos de acesso do Outposts), escolha a guia Outposts endpoints (Endpoints do Outposts).
4. Em Outposts endpoints (Endpoints do Outposts), você pode visualizar uma lista de endpoints do S3 on Outposts.

Como usar o AWS CLI

O exemplo a seguir da AWS CLI lista os endpoints para os recursos do AWS Outposts associados à sua conta. Para obter mais informações sobre esse comando, consulte list-endpoints na Referência da AWS CLI.

```
aws s3outposts list-endpoints
```

Usar o AWS SDK para Java

O exemplo do SDK para Java a seguir lista os endpoints para um Outpost. Para obter mais informações, consulte ListEndpoints na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.ListEndpointsRequest;
import com.amazonaws.services.s3outposts.model.ListEndpointsResult;

public void listEndpoints() {
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder
                .standard().build();

    ListEndpointsRequest listEndpointsRequest = new ListEndpointsRequest();
    ListEndpointsResult listEndpointsResult =
 s3OutpostsClient.listEndpoints(listEndpointsRequest);
    System.out.println("List endpoints result is " + listEndpointsResult);
}
```

Excluir um endpoint do Amazon S3 on Outposts

Para rotear solicitações para um ponto de acesso do Amazon S3 on Outposts, você deve criar e configurar um endpoint do S3 on Outposts. Para criar um endpoint, você precisará de uma conexão ativa com seu link de serviço com sua região de origem do Outposts. Cada nuvem privada virtual (VPC) em seu Outpost pode ter um endpoint associado. Para obter mais informações sobre cotas de endpoints, consulte Requisitos de rede do S3 on Outposts. Você deve criar um endpoint para poder acessar seus buckets do Outposts e executar operações de objeto. Para obter mais informações, consulte Endpoints.

Os exemplos a seguir mostram como excluir os endpoints do S3 on Outposts usando o Console de gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts access points (Pontos de acesso do Outposts).
3. Na página Outposts access points (Pontos de acesso do Outposts), escolha a guia Outposts endpoints (Endpoints do Outposts).
4. Em Outposts endpoints (Endpoints do Outposts), escolha o endpoint que você deseja excluir e escolha Delete (Excluir).

Como usar o AWS CLI

O exemplo da AWS CLI a seguir exclui um endpoint de um Outpost. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3outposts delete-endpoint --endpoint-id example-endpoint-id --outpost-
id op-01ac5d28a6a232904
```

Usar o AWS SDK para Java

O exemplo do SDK for Java a seguir exclui um endpoint de um Outpost. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
import com.amazonaws.arn.Arn;
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
```

```
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.DeleteEndpointRequest;

public void deleteEndpoint(String endpointArnInput) {
    String outpostId = "op-01ac5d28a6a232904";
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder
                .standard().build();

    Arn endpointArn = Arn.fromString(endpointArnInput);
    String[] resourceParts = endpointArn.getResource().getResource().split("/");
    String endpointId = resourceParts[resourceParts.length - 1];
    DeleteEndpointRequest deleteEndpointRequest = new DeleteEndpointRequest()
                .withEndpointId(endpointId)
                .withOutpostId(outpostId);
    s3OutpostsClient.deleteEndpoint(deleteEndpointRequest);
    System.out.println("Endpoint with id " + endpointId + " is deleted.");
}
```

Trabalhar com objetos usando o S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (0UTP0STS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST.

Objetos são as entidades fundamentais armazenadas no Amazon S3 on Outposts. Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outpost. Ao especificar o bucket para operações de objeto, use o nome do recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 no Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

Os ARNs de objeto usam o formato a seguir, que inclui a Região da AWS na qual está o Outpost, o ID da Conta da AWS, o ID do Outpost, o nome do bucket e a chave do objeto:

```
arn:aws:s3-outposts:us-west-2:123456789012:outpost/ op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1/object/myobject
```

Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos

requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Tópicos

- Fazer upload de um objeto em um bucket do S3 on Outposts
- Copiar um objeto em um bucket do Amazon S3 no Outposts usando o AWS SDK para Java
- Obter um objeto de um bucket do Amazon S3 on Outposts
- Listar os objetos em um bucket do Amazon S3 on Outposts
- Excluir objetos em buckets do Amazon S3 on Outposts
- Usar o HeadBucket para determinar se existe um bucket do S3 on Outposts e se você tem permissões de acesso
- Realizar e gerenciar um carregamento fracionado com o SDK para Java
- Uso de URLs pré-assinados para o S3 no Outposts
- Amazon S3 no Outposts com Amazon EMR no Outposts local
- Armazenamento em cache de autorização e autenticação

Fazer upload de um objeto em um bucket do S3 on Outposts

Objetos são as entidades fundamentais armazenadas no Amazon S3 on Outposts. Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outpost. Ao especificar o bucket para operações de objeto, use o nome do recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 no Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Os exemplos de AWS CLI e AWS SDK para Java a seguir mostram como fazer upload de um objeto em um bucket do S3 on Outposts usando um ponto de acesso.

AWS CLI

Example

O exemplo a seguir coloca um objeto chamado `sample-object.xml` em um bucket do S3 on Outposts (`s3-outposts:PutObject`) usando a AWS CLI. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte put-object na Referência da AWS CLI.

```
aws s3api put-object --bucket arn:aws:s3-
outposts:Region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --key sample-object.xml --body sample-object.xml
```

SDK for Java

Example

Para ver exemplos de como fazer upload de um objeto em um bucket do S3 Outposts com o AWS SDK para Java, consulte PutObjectOnOutpost.java nos exemplos de código do AWSSDK para Java 2.x.

Copiar um objeto em um bucket do Amazon S3 no Outposts usando o AWS SDK para Java

Objetos são as entidades fundamentais armazenadas no Amazon S3 on Outposts. Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um

bucket do Outpost. Ao especificar o bucket para operações de objeto, use o nome do recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 no Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Os exemplos a seguir mostram como copiar um objeto em um bucket do S3 on Outposts usando o AWS SDK para Java.

Usar o AWS SDK para Java

O exemplo do S3 on Outposts a seguir copia um objeto para um novo objeto no mesmo bucket usando o SDK para Java. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;

public class CopyObject {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
```

```
        String sourceKey = "*** Source object key ***";
        String destinationKey = "*** Destination object key ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(accessPointArn,
 sourceKey, accessPointArn, destinationKey);
            s3Client.copyObject(copyObjectRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Obter um objeto de um bucket do Amazon S3 on Outposts

Objetos são as entidades fundamentais armazenadas no Amazon S3 on Outposts. Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outpost. Ao especificar o bucket para operações de objeto, use o nome do recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 no Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Os exemplos a seguir mostram como baixar (get) um objeto usando a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Como usar o AWS CLI

O exemplo a seguir obtém um objeto chamado `sample-object.xml` de um bucket do S3 on Outposts (`s3-outposts:GetObject`) usando a AWS CLI. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte get-object na Referência de comandos da AWS CLI.

```
aws s3api get-object --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point --key testkey sample-object.xml
```

Usar o AWS SDK para Java

O exemplo do S3 on Outposts a seguir obtém um objeto usando o SDK para Java. Para usar esse exemplo, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações, consulte GetObject na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GetObjectRequest;
import com.amazonaws.services.s3.model.ResponseHeaderOverrides;
import com.amazonaws.services.s3.model.S3Object;

import java.io.BufferedReader;
import java.io.IOException;
```

```
import java.io.InputStream;
import java.io.InputStreamReader;

public class GetObject {
    public static void main(String[] args) throws IOException {
        String accessPointArn = "*** access point ARN ***";
        String key = "*** Object key ***";

        S3Object fullObject = null, objectPortion = null, headerOverrideObject = null;
        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Get an object and print its contents.
            System.out.println("Downloading an object");
            fullObject = s3Client.getObject(new GetObjectRequest(accessPointArn, key));
            System.out.println("Content-Type: " +
 fullObject.getObjectMetadata().getContentType());
            System.out.println("Content: ");
            displayTextInputStream(fullObject.getObjectContent());

            // Get a range of bytes from an object and print the bytes.
            GetObjectRequest rangeObjectRequest = new GetObjectRequest(accessPointArn,
 key)
                    .withRange(0, 9);
            objectPortion = s3Client.getObject(rangeObjectRequest);
            System.out.println("Printing bytes retrieved.");
            displayTextInputStream(objectPortion.getObjectContent());

            // Get an entire object, overriding the specified response headers, and
 print the object's content.
            ResponseHeaderOverrides headerOverrides = new ResponseHeaderOverrides()
                    .withCacheControl("No-cache")
                    .withContentDisposition("attachment; filename=example.txt");
            GetObjectRequest getObjectRequestHeaderOverride = new
 GetObjectRequest(accessPointArn, key)
                    .withResponseHeaders(headerOverrides);
            headerOverrideObject = s3Client.getObject(getObjectRequestHeaderOverride);
            displayTextInputStream(headerOverrideObject.getObjectContent());
        } catch (AmazonServiceException e) {
```

```
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        } finally {
            // To ensure that the network connection doesn't remain open, close any
 open input streams.
            if (fullObject != null) {
                fullObject.close();
            }
            if (objectPortion != null) {
                objectPortion.close();
            }
            if (headerOverrideObject != null) {
                headerOverrideObject.close();
            }
        }
    }

    private static void displayTextInputStream(InputStream input) throws IOException {
        // Read the text input stream one line at a time and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line = null;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

Listar os objetos em um bucket do Amazon S3 on Outposts

Objetos são as entidades fundamentais armazenadas no Amazon S3 on Outposts. Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outpost. Ao especificar o bucket para operações de objeto, use o nome do recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 no Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

> **Note**
>
> Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Os exemplos a seguir mostram como listar os objetos em um bucket do S3 on Outposts usando a AWS CLI e o AWS SDK para Java.

Uso do AWS CLI

O exemplo a seguir lista os objetos em um bucket do S3 on Outposts (`s3-outposts:ListObjectsV2`) usando a AWS CLI. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte list-objects-v2 na Referência da AWS CLI.

```
aws s3api list-objects-v2 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-access-point
```

> **Note**
>
> Ao usar essa ação com o Amazon S3 on Outposts por meio de AWS SDKs, forneça o ARN do ponto de acesso do Outposts no lugar do nome do bucket, no seguinte formato:

`arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-Outposts-Access-Point`. Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

Usar o AWS SDK para Java

O exemplo do S3 on Outposts a seguir lista objetos em um bucket usando o SDK para Java. Para usar esse exemplo, substitua cada *user input placeholder* por suas próprias informações.

Important

Este exemplo usa ListObjectsV2, que é a última revisão da operação `ListObjects` da API. Recomendamos que você use essa operação de API revisada para o desenvolvimento de aplicações. Para compatibilidade com versões anteriores, o Amazon S3 continua a oferecer suporte à versão anterior desta operação de API.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListObjectsV2Request;
import com.amazonaws.services.s3.model.ListObjectsV2Result;
import com.amazonaws.services.s3.model.S3ObjectSummary;

public class ListObjectsV2 {

    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            System.out.println("Listing objects");
```

```
            // maxKeys is set to 2 to demonstrate the use of
            // ListObjectsV2Result.getNextContinuationToken()
            ListObjectsV2Request req = new
 ListObjectsV2Request().withBucketName(accessPointArn).withMaxKeys(2);
            ListObjectsV2Result result;

            do {
                result = s3Client.listObjectsV2(req);

                for (S3ObjectSummary objectSummary : result.getObjectSummaries()) {
                    System.out.printf(" - %s (size: %d)\n", objectSummary.getKey(),
 objectSummary.getSize());
                }
                // If there are more than maxKeys keys in the bucket, get a
 continuation token
                // and list the next objects.
                String token = result.getNextContinuationToken();
                System.out.println("Next Continuation Token: " + token);
                req.setContinuationToken(token);
            } while (result.isTruncated());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Excluir objetos em buckets do Amazon S3 on Outposts

Objetos são as entidades fundamentais armazenadas no Amazon S3 on Outposts. Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outpost. Ao especificar o bucket para operações de objeto, use o nome do recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 no Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Os exemplos a seguir mostram como excluir um ou vários objetos em um bucket do S3 on Outposts usando a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Uso do AWS CLI

Os exemplos a seguir mostram como excluir um único ou vários objetos de um bucket do S3 on Outposts.

delete-object

O exemplo a seguir exclui um objeto chamado `sample-object.xml` de um bucket do S3 on Outposts (`s3-outposts:DeleteObject`) usando a AWS CLI. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte delete-object na Referência de comandos da AWS CLI.

```
aws s3api delete-object --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --key sample-object.xml
```

delete-objects

O exemplo a seguir exclui dois objetos chamados `sample-object.xml` e `test1.text` de um bucket do S3 on Outposts (`s3-outposts:DeleteObject`) usando a AWS CLI. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte delete-objects na Referência de comandos da AWS CLI.

```
aws s3api delete-objects --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --delete file://delete.json

delete.json
{
  "Objects": [
    {
      "Key": "test1.txt"
    },
    {
      "Key": "sample-object.xml"
    }
  ],
  "Quiet": false
}
```

Usar o AWS SDK para Java

Os exemplos a seguir mostram como excluir um único ou vários objetos de um bucket do S3 on Outposts.

DeleteObject

O exemplo do S3 on Outposts a seguir exclui um objeto de um bucket usando o SDK para Java. Para usar este exemplo, especifique o ARN do ponto de acesso para o Outpost e o nome da chave para o objeto que você deseja excluir. Para obter mais informações, consulte DeleteObject na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
```

```
import com.amazonaws.services.s3.model.DeleteObjectRequest;

public class DeleteObject {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String keyName = "*** key name ****";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            s3Client.deleteObject(new DeleteObjectRequest(accessPointArn, keyName));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

DeleteObjects

O exemplo do S3 on Outposts a seguir faz upload e depois exclui objetos de um bucket usando o SDK para Java. Para usar este exemplo, especifique o ARN do ponto de acesso para o Outpost. Para obter mais informações, consulte DeleteObjects na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectsRequest;
import com.amazonaws.services.s3.model.DeleteObjectsRequest.KeyVersion;
import com.amazonaws.services.s3.model.DeleteObjectsResult;
```

```
import java.util.ArrayList;

public class DeleteObjects {

    public static void main(String[] args) {
       String accessPointArn = "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point";


        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Upload three sample objects.
            ArrayList<KeyVersion> keys = new ArrayList<KeyVersion>();
            for (int i = 0; i < 3; i++) {
                String keyName = "delete object example " + i;
                s3Client.putObject(accessPointArn, keyName, "Object number " + i + "
 to be deleted.");
                keys.add(new KeyVersion(keyName));
            }
            System.out.println(keys.size() + " objects successfully created.");

            // Delete the sample objects.
            DeleteObjectsRequest multiObjectDeleteRequest = new
 DeleteObjectsRequest(accessPointArn)
                    .withKeys(keys)
                    .withQuiet(false);

            // Verify that the objects were deleted successfully.
            DeleteObjectsResult delObjRes =
 s3Client.deleteObjects(multiObjectDeleteRequest);
            int successfulDeletes = delObjRes.getDeletedObjects().size();
            System.out.println(successfulDeletes + " objects successfully
 deleted.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
```

```
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Usar o HeadBucket para determinar se existe um bucket do S3 on Outposts e se você tem permissões de acesso

Objetos são as entidades fundamentais armazenadas no Amazon S3 on Outposts. Cada objeto está contido em um bucket. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outpost. Ao especificar o bucket para operações de objeto, use o nome do recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso. Para obter mais informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O exemplo a seguir mostra o formato do ARN para pontos de acesso do S3 no Outposts, que inclui o código Região da AWS para a região em que o Outpost está hospedado, o ID da Conta da AWS, o ID do Outpost e o nome do ponto de acesso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obter mais informações sobre o S3 on Outposts, consulte ARNs de recurso para S3 no Outposts.

> **Note**
>
> Com o Amazon S3 on Outposts, os dados do objeto são sempre armazenados no Outpost. Quando a AWS instala um rack do Outpost, seus dados permanecem no local do Outpost para atender aos requisitos de residência de dados. Seus objetos nunca saem do Outpost e não estão em uma Região da AWS. Como o Console de gerenciamento da AWS está hospedado na região, você não pode usá-lo para fazer upload de objetos no Outpost nem os gerenciar. No entanto, você pode usar a API REST, a AWS Command Line Interface (AWS CLI) e os SDKs para fazer upload de objetos e gerenciá-los por meio de seus pontos de acesso.

Os exemplos de AWS Command Line Interface (AWS CLI) e AWS SDK para Java a seguir mostram como usar a operação HeadBucket da API para determinar se existe um bucket do Amazon S3 on Outposts e se você tem permissão para acessá-lo. Para obter mais informações, consulte HeadBucket na Referência de API do Amazon Simple Storage Service.

Como usar o AWS CLI

O exemplo de AWS CLI do S3 no Outposts a seguir usa o comando `head-bucket` para determinar se existe um bucket e se você tem permissão para acessá-lo. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte head-bucket na Referência da AWS CLI.

```
aws s3api head-bucket --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

Usar o AWS SDK para Java

O exemplo do S3 on Outposts a seguir mostra como determinar se existe um bucket e se você tem permissão para acessá-lo. Para usar este exemplo, especifique o ARN do ponto de acesso para o Outpost. Para obter mais informações, consulte HeadBucket na Referência de API do Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.HeadBucketRequest;

public class HeadBucket {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();
```

```
            s3Client.headBucket(new HeadBucketRequest(accessPointArn));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Realizar e gerenciar um carregamento fracionado com o SDK para Java

Com o Amazon S3 on Outposts, é possível criar buckets do S3 em seus recursos do AWS Outposts, além de armazenar e recuperar objetos no ambiente on-premises para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Os exemplos a seguir mostram como usar o S3 on Outposts com o AWS SDK para Java para executar e gerenciar um carregamento fracionado.

Tópicos

- Efetuar o upload fracionado de um objeto em um bucket do Amazon S3 on Outposts
- Copiar um objeto grande em um bucket do S3 on Outposts usando carregamento fracionado
- Listar partes de um objeto em um bucket do S3 no Outposts
- Recuperar uma lista de multipart uploads em andamento em um bucket do S3 no Outposts

Efetuar o upload fracionado de um objeto em um bucket do Amazon S3 on Outposts

O exemplo do S3 on Outposts a seguir inicia, faz upload e conclui um carregamento fracionado em um bucket usando o SDK para Java. Para usar esse exemplo, substitua cada *`user input`*

placeholder por suas próprias informações. Consulte mais informações em Fazer upload de um objeto usando multipart upload no Guia do usuário do Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.ArrayList;
import java.util.List;

public class MultipartUploadCopy {
    public static void main(String[] args) {
        String accessPointArn = "*** Source access point ARN ***";
        String sourceObjectKey = "*** Source object key ***";
        String destObjectKey = "*** Target object key ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(accessPointArn, destObjectKey);
            InitiateMultipartUploadResult initResult =
 s3Client.initiateMultipartUpload(initRequest);

            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
 GetObjectMetadataRequest(accessPointArn, sourceObjectKey);
            ObjectMetadata metadataResult =
 s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
```

```
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(accessPointArn)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(accessPointArn)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }

            // Complete the upload request to concatenate all uploaded parts and make
the copied object available.
            CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest(
                    accessPointArn,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
```

```
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
```

Copiar um objeto grande em um bucket do S3 on Outposts usando carregamento fracionado

O exemplo do S3 on Outposts a seguir usa o SDK para Java para copiar um objeto em um bucket. Para usar esse exemplo, substitua cada *`user input placeholder`* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.ArrayList;
import java.util.List;

public class MultipartUploadCopy {
    public static void main(String[] args) {
        String accessPointArn = "*** Source access point ARN ***";
        String sourceObjectKey = "*** Source object key ***";
        String destObjectKey = "*** Target object key ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(accessPointArn, destObjectKey);
            InitiateMultipartUploadResult initResult =
 s3Client.initiateMultipartUpload(initRequest);
```

```
            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest(accessPointArn, sourceObjectKey);
            ObjectMetadata metadataResult =
s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(accessPointArn)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(accessPointArn)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }

            // Complete the upload request to concatenate all uploaded parts and make
the copied object available.
            CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest(
                    accessPointArn,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
```

```
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
}
```

Listar partes de um objeto em um bucket do S3 no Outposts

O exemplo do S3 on Outposts a seguir lista as partes de um objeto em um bucket usando o SDK para Java. Para usar esse exemplo, substitua cada *`user input placeholder`* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.List;

public class ListParts {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String keyName = "*** Key name ***";
        String uploadId = "*** Upload ID ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
```

```
                    .enableUseArnRegion()
                    .build();

            ListPartsRequest listPartsRequest = new ListPartsRequest(accessPointArn,
 keyName, uploadId);
            PartListing partListing = s3Client.listParts(listPartsRequest);
            List<PartSummary> partSummaries = partListing.getParts();

            System.out.println(partSummaries.size() + " multipart upload parts");
            for (PartSummary p : partSummaries) {
                System.out.println("Upload part: Part number = \"" + p.getPartNumber()
 + "\", ETag = " + p.getETag());
            }

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Recuperar uma lista de multipart uploads em andamento em um bucket do S3 no Outposts

O exemplo do S3 on Outposts a seguir mostra como recuperar uma lista de carregamentos fracionados em andamento de um bucket do Outposts usando o SDK para Java. Para usar esse exemplo, substitua cada *`user input placeholder`* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListMultipartUploadsRequest;
import com.amazonaws.services.s3.model.MultipartUpload;
import com.amazonaws.services.s3.model.MultipartUploadListing;

import java.util.List;
```

```
public class ListMultipartUploads {
    public static void main(String[] args) {
                String accessPointArn = "*** access point ARN ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Retrieve a list of all in-progress multipart uploads.
            ListMultipartUploadsRequest allMultipartUploadsRequest = new
 ListMultipartUploadsRequest(accessPointArn);
            MultipartUploadListing multipartUploadListing =
 s3Client.listMultipartUploads(allMultipartUploadsRequest);
            List<MultipartUpload> uploads =
 multipartUploadListing.getMultipartUploads();

            // Display information about all in-progress multipart uploads.
            System.out.println(uploads.size() + " multipart upload(s) in progress.");
            for (MultipartUpload u : uploads) {
                System.out.println("Upload in progress: Key = \"" + u.getKey() + "\",
 id = " + u.getUploadId());
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Uso de URLs pré-assinados para o S3 no Outposts

Você pode usar um URL pré-assinado para conceder acesso por tempo limitado a objetos armazenados localmente em um Outpost sem atualizar sua política de bucket. Com URLs pré-

assinados, como proprietário do bucket, você pode compartilhar objetos com indivíduos em sua nuvem privada virtual (VPC) ou conceder a eles a capacidade de carregar ou excluir objetos.

Ao criar um URL pré-assinado usando os AWS SDKs ou a AWS Command Line Interface (AWS CLI), você associa o URL a uma ação específica. Você também concede acesso por tempo limitado ao URL pré-assinado escolhendo um tempo de expiração personalizado a partir de 1 segundo e de até 7 dias. Ao compartilhar o URL pré-assinado, o indivíduo na VPC pode executar a ação incorporada no URL como se fosse o usuário da assinatura original. Ao atingir o tempo de expiração, o URL expira e não funciona mais.

Limitar recursos de pre-signed URLs

Os recursos de um URL pré-assinado são limitados pelas permissões do usuário que o criou. Em essência, os URLs pré-assinados são tokens ao portador que concedem acesso ao portador. Dessa forma, recomendamos que você os proteja adequadamente.

AWS Signature Version 4 (SigV4)

Para aplicar um comportamento específico quando solicitações de URL pré-assinado forem autenticadas usando AWS Signature Version 4 (SigV4), você pode usar chaves de condição nas políticas de bucket e políticas de ponto de acesso. Por exemplo, você pode criar uma política de bucket que use a condição `s3-outposts:signatureAge` para negar qualquer solicitação de URL pré-assinado do Amazon S3 no Outposts em objetos no bucket `example-outpost-bucket` se a assinatura tiver mais de 10 minutos de idade. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Deny a presigned URL request if the signature is more than 10
 minutes old",
            "Effect": "Deny",
            "Principal": {"AWS":"444455556666"},
            "Action": "s3-outposts:*",
            "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
```

```
            "Condition": {
                "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
                "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
            }
        }
    ]
}
```

Para obter uma lista de chaves de condição e exemplos adicionais de política que você pode usar para aplicar um comportamento específico quando solicitações de URL pré-assinado forem autenticadas usando o Signature Version 4, consulte Chaves de política específicas de autenticação do AWS Signature Version 4 (SigV4).

Restrição de caminho de rede

Se quiser restringir o uso de URLs pré-assinados e qualquer acesso do S3 no Outposts a caminhos específicos de rede, você poderá criar políticas que exijam um caminho específico de rede. Para definir a restrição na entidade principal do IAM que faz a chamada, você pode usar políticas do AWS Identity and Access Management (IAM) baseadas em identidade (por exemplo, políticas de usuário, grupo ou perfil). Para definir a restrição no recurso do S3 no Outposts, você pode usar políticas baseadas em recursos (p. ex., políticas de bucket e ponto de acesso).

Uma restrição de caminho de rede na entidade principal do IAM exige que o usuário dessas credenciais faça solicitações pela rede especificada. Uma restrição no bucket ou no ponto de acesso exige que todas as solicitações encaminhadas para esse recurso tenham origem na rede especificada. Essas restrições também são aplicadas fora do cenário de URL pré-assinado.

A condição global do IAM que você usa depende do tipo de endpoint. Se estiver usando o endpoint público para o S3 no Outposts, use `aws:SourceIp`. Se estiver usando um endpoint da VPC para o S3 no Outposts, use `aws:SourceVpc` ou `aws:SourceVpce`.

A declaração de política do IAM a seguir requer que a entidade principal só acesse a AWS do intervalo de rede especificado. Com essa declaração de política, exige-se que qualquer acesso tenha origem nesse intervalo. Isso inclui o caso de alguém que esteja usando um URL pré-assinado para o S3 no Outposts. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
{
    "Sid": "NetworkRestrictionForIAMPrincipal",
```

```
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
        "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
        "BoolIfExists": {"aws:ViaAWSService": "false"}
    }
}
```

Para ver um exemplo de política de bucket que usa a chave de condição global `aws:SourceIP` da AWS para restringir o acesso a um bucket do S3 no Outposts a um intervalo específico de rede, consulte Configurar o IAM com o S3 on Outposts.

Quem pode criar um URL pré-assinado

Qualquer um com credenciais de segurança válidas pode criar um pre-signed URL. Porém, para que um usuário na VPC tenha êxito no acesso a um objeto, o URL pré-assinado deve ter sido criado por alguém que tenha permissão para executar a operação na qual o URL pré-assinado é baseado.

Você pode usar as seguintes credenciais para criar um URL pré-assinado:

- Perfil de instância do IAM: válido por até 6 horas.
- AWS Security Token Service: válido por até 36 horas quando assinado com credenciais permanentes, como as credenciais do usuário raiz da Conta da AWS ou um usuário do IAM.
- Usuário do IAM: válido por até 7 dias quando você estiver usando o AWS Signature Version 4.

  Para criar um URL pré-assinado que seja válido por até 7 dias, primeiro delegue credenciais de usuário do IAM (a chave de acesso e a chave secreta) ao SDK que estiver usando. Em seguida, gere um URL pré-assinado usando o AWS Signature Version 4.

> **Note**
>
> - Se tiver criado um URL pré-assinado usando um token temporário, o URL expirará quando o token expirar, mesmo que você tenha criado o URL com um tempo de expiração posterior.
> - Como os URLs pré-assinados concedem acesso aos seus buckets do S3 no Outposts a quem tiver o URL, recomendamos protegê-los adequadamente. Para obter mais

informações sobre como proteger URLs pré-assinados, consulte Limitar recursos de pre-signed URLs.

Quando o S3 no Outposts confere a data e a hora de validade de um URL pré-assinado?

O S3 no Outposts confere a data e a hora de expiração de um URL assinado ao receber a solicitação HTTP. Por exemplo, se um cliente começar a baixar um arquivo grande imediatamente antes do tempo de expiração, o download continuará mesmo que o tempo de expiração acabe durante o download. No entanto, se a conexão cair e o cliente tentar reiniciar o download posteriormente ao término do tempo de expiração, o download vai falhar.

Para obter mais informações sobre como usar um URL pré-assinado para compartilhar ou carregar objetos, consulte os tópicos a seguir.

Tópicos

- Compartilhar objetos usando URLs pré-assinados
- Gerar um URL pré-assinado para carregar um objeto em um bucket do S3 no Outposts

Compartilhar objetos usando URLs pré-assinados

Você pode usar um URL pré-assinado para conceder acesso por tempo limitado a objetos armazenados localmente em um Outpost sem atualizar sua política de bucket. Com URLs pré-assinados, como proprietário do bucket, você pode compartilhar objetos com indivíduos em sua nuvem privada virtual (VPC) ou conceder a eles a capacidade de carregar ou excluir objetos.

Ao criar um URL pré-assinado usando os AWS SDKs ou a AWS Command Line Interface (AWS CLI), você associa o URL a uma ação específica. Você também concede acesso por tempo limitado ao URL pré-assinado escolhendo um tempo de expiração personalizado a partir de 1 segundo e de até 7 dias. Ao compartilhar o URL pré-assinado, o indivíduo na VPC pode executar a ação incorporada no URL como se fosse o usuário da assinatura original. Ao atingir o tempo de expiração, o URL expira e não funciona mais.

Ao criar um URL pré-assinado, você deve fornecer suas credenciais de segurança e especificar o seguinte:

- Um nome do recurso da Amazon (ARN) de ponto de acesso para o bucket do Amazon S3 no Outposts
- Uma chave de objeto
- Um método HTTP (`GET` para baixar objetos)
- Data e hora de expiração

Os URLs pré-assinados só são válidos pela duração especificada. Ou seja, é necessário iniciar a ação permitida pelo URL antes da data e da hora de expiração. É possível usar o URL pré-assinado várias vezes até a data e a hora de expiração. Se tiver criado um URL pré-assinado usando um token temporário, o URL expirará quando o token expirar, mesmo que você tenha criado o URL com um tempo de expiração posterior.

Os usuários na nuvem privada virtual (VPC) que tiverem acesso ao URL pré-assinado poderão acessar o objeto. Por exemplo, se você tiver um vídeo em seu bucket e o bucket e o objeto forem privados, será possível compartilhar o vídeo gerando um pre-signed URL. Como os URLs pré-assinados concedem acesso aos seus buckets do S3 no Outposts a quem tiver o URL, recomendamos proteger os URLs adequadamente. Para obter mais detalhes sobre como proteger pre-signed URLs, consulte Limitar recursos de pre-signed URLs.

Qualquer um com credenciais de segurança válidas pode criar um pre-signed URL. No entanto, o URL pré-assinado deve ter sido criado por alguém que tenha permissão para executar a operação na qual o URL pré-assinado é baseado. Para obter mais informações, consulte Quem pode criar um URL pré-assinado.

É possível gerar um URL pré-assinado para compartilhar um objeto em um bucket do S3 no Outposts usando os AWS SDKs e a AWS CLI. Para obter mais informações, veja os exemplos a seguir:

Usar SDKs da AWS

Você pode usar os AWS SDKs para gerar um URL pré-assinado que você pode compartilhar com terceiros para que eles recuperem um objeto.

> **Note**
>
> Ao usar os AWS SDKs para gerar um URL pré-assinado, o tempo máximo de expiração de um URL pré-assinado é de sete dias a partir do momento da criação.

Java

Example

O exemplo a seguir gera um URL pré-assinado que você pode compartilhar com terceiros para que eles recuperem um objeto de um bucket do S3 no Outposts. Para obter mais informações, consulte Uso de URLs pré-assinados para o S3 no Outposts. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.HttpMethod;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GeneratePresignedUrlRequest;

import java.io.IOException;
import java.net.URL;
import java.time.Instant;

public class GeneratePresignedURL {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String accessPointArn = "*** access point ARN ***";
        String objectKey = "*** object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Set the presigned URL to expire after one hour.
            java.util.Date expiration = new java.util.Date();
            long expTimeMillis = Instant.now().toEpochMilli();
            expTimeMillis += 1000 * 60 * 60;
            expiration.setTime(expTimeMillis);

            // Generate the presigned URL.
            System.out.println("Generating pre-signed URL.");
```

```
            GeneratePresignedUrlRequest generatePresignedUrlRequest =
                    new GeneratePresignedUrlRequest(accessPointArn, objectKey)
                            .withMethod(HttpMethod.GET)
                            .withExpiration(expiration);
            URL url = s3Client.generatePresignedUrl(generatePresignedUrlRequest);

            System.out.println("Pre-Signed URL: " + url.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't
 process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Example

O exemplo a seguir gera um URL pré-assinado que você pode compartilhar com terceiros para que eles recuperem um objeto de um bucket do S3 no Outposts. Para obter mais informações, consulte Uso de URLs pré-assinados para o S3 no Outposts. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;

namespace Amazon.DocSamples.S3
{
    class GenPresignedURLTest
    {
        private const string accessPointArn = "*** access point ARN ***";
        private const string objectKey = "*** object key ***";
        // Specify how long the presigned URL lasts, in hours.
        private const double timeoutDuration = 12;
```

```
        // Specify your bucket Region (an example Region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            string urlString = GeneratePreSignedURL(timeoutDuration);
        }
        static string GeneratePreSignedURL(double duration)
        {
            string urlString = "";
            try
            {
                GetPreSignedUrlRequest request1 = new GetPreSignedUrlRequest
                {
                    BucketName = accessPointArn,
                    Key = objectKey,
                    Expires = DateTime.UtcNow.AddHours(duration)
                };
                urlString = s3Client.GetPreSignedURL(request1);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            return urlString;
        }
    }
}
```

Python

O exemplo a seguir gera um URL pré-assinado para compartilhar um objeto usando o SDK para Python (Boto3). Por exemplo, use um cliente Boto3 e a função `generate_presigned_url` para gerar um URL pré-assinado que permite a fazer realizar o `GET` em um objeto.

```
import boto3
    url = boto3.client('s3').generate_presigned_url(
    ClientMethod='get_object',
    Params={'Bucket': 'ACCESS_POINT_ARN', 'Key': 'OBJECT_KEY'},
    ExpiresIn=3600)
```

Para obter mais informações sobre como usar o SDK para Python (Boto3) para gerar um URL pré-assinado, consulte Python na Referência de API do AWS SDK para Python (Boto).

Como usar o AWS CLI

O seguinte exemplo de comando da AWS CLI gera um URL pré-assinado para um bucket do S3 no Outposts. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

> **Note**
>
> Ao usar a AWS CLI para gerar um URL pré-assinado, o tempo máximo de expiração de um URL pré-assinado é de sete dias a partir do momento da criação.

```
aws s3 presign s3://arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/example-outpost-access-
point/mydoc.txt --expires-in 604800
```

Para obter mais informações, consulte presign (pré-assinatura) na Referência de comandos da AWS CLI.

Gerar um URL pré-assinado para carregar um objeto em um bucket do S3 no Outposts

Você pode usar um URL pré-assinado para conceder acesso por tempo limitado a objetos armazenados localmente em um Outpost sem atualizar sua política de bucket. Com URLs pré-assinados, como proprietário do bucket, você pode compartilhar objetos com indivíduos em sua nuvem privada virtual (VPC) ou conceder a eles a capacidade de carregar ou excluir objetos.

Ao criar um URL pré-assinado usando os AWS SDKs ou a AWS Command Line Interface (AWS CLI), você associa o URL a uma ação específica. Você também concede acesso por tempo limitado

ao URL pré-assinado escolhendo um tempo de expiração personalizado a partir de 1 segundo e de até 7 dias. Ao compartilhar o URL pré-assinado, o indivíduo na VPC pode executar a ação incorporada no URL como se fosse o usuário da assinatura original. Ao atingir o tempo de expiração, o URL expira e não funciona mais.

Ao criar um URL pré-assinado, você deve fornecer suas credenciais de segurança e especificar o seguinte:

- Um nome do recurso da Amazon (ARN) de ponto de acesso para o bucket do Amazon S3 no Outposts
- Uma chave de objeto
- Um método HTTP (PUT para carregar objetos)
- Data e hora de expiração

Os URLs pré-assinados só são válidos pela duração especificada. Ou seja, é necessário iniciar a ação permitida pelo URL antes da data e da hora de expiração. É possível usar o URL pré-assinado várias vezes até a data e a hora de expiração. Se tiver criado um URL pré-assinado usando um token temporário, o URL expirará quando o token expirar, mesmo que você tenha criado o URL com um tempo de expiração posterior.

Se a ação permitida por um URL pré-assinado consistir em várias etapas, como um multipart upload, é necessário iniciar todas as etapas antes do tempo de expiração. Você receberá um erro se o S3 no Outposts tentar iniciar uma etapa com um URL expirado.

Os usuários na nuvem privada virtual (VPC) que tiverem acesso ao URL pré-assinado poderão carregar objetos. Por exemplo, um usuário na VPC que tenha acesso ao URL pré-assinado pode carregar um objeto para o seu bucket. Como os URLs pré-assinados concedem acesso aos seus buckets do S3 no Outposts a qualquer usuário na VPC que tenha acesso ao URL pré-assinado, recomendamos proteger esses URLs adequadamente. Para obter mais detalhes sobre como proteger pre-signed URLs, consulte Limitar recursos de pre-signed URLs.

Qualquer um com credenciais de segurança válidas pode criar um pre-signed URL. No entanto, o URL pré-assinado deve ter sido criado por alguém que tenha permissão para executar a operação na qual o URL pré-assinado é baseado. Para obter mais informações, consulte Quem pode criar um URL pré-assinado.

Usar os AWS SDKs para gerar um URL pré-assinado para uma operação de objeto do S3 no Outposts

Java

SDK para Java 2.x

Este exemplo mostra como gerar um URL pré-assinado que você pode usar para carregar um objeto em um bucket do S3 no Outposts por um tempo limitado. Para obter mais informações, consulte Uso de URLs pré-assinados para o S3 no Outposts.

```
   public static void signBucket(S3Presigner presigner, String
outpostAccessPointArn, String keyName) {

       try {
           PutObjectRequest objectRequest = PutObjectRequest.builder()
                   .bucket(accessPointArn)
                   .key(keyName)
                   .contentType("text/plain")
                   .build();

           PutObjectPresignRequest presignRequest =
PutObjectPresignRequest.builder()
                   .signatureDuration(Duration.ofMinutes(10))
                   .putObjectRequest(objectRequest)
                   .build();

           PresignedPutObjectRequest presignedRequest =
presigner.presignPutObject(presignRequest);


           String myURL = presignedRequest.url().toString();
           System.out.println("Presigned URL to upload a file to: " +myURL);
           System.out.println("Which HTTP method must be used when uploading a
file: " +
                   presignedRequest.httpRequest().method());

           // Upload content to the S3 on Outposts bucket by using this URL.
           URL url = presignedRequest.url();

           // Create the connection and use it to upload the new object by using
the presigned URL.
```

```
            HttpURLConnection connection = (HttpURLConnection)
 url.openConnection();
            connection.setDoOutput(true);
            connection.setRequestProperty("Content-Type","text/plain");
            connection.setRequestMethod("PUT");
            OutputStreamWriter out = new
 OutputStreamWriter(connection.getOutputStream());
            out.write("This text was uploaded as an object by using a presigned
 URL.");
            out.close();

            connection.getResponseCode();
            System.out.println("HTTP response code is " +
 connection.getResponseCode());

        } catch (S3Exception e) {
            e.getStackTrace();
        } catch (IOException e) {
            e.getStackTrace();
        }
    }
```

Python

SDK para Python (Boto3).

Este exemplo mostra como gerar um URL pré-assinado que pode executar uma ação do S3 no Outposts por um tempo limitado. Para obter mais informações, consulte Uso de URLs pré-assinados para o S3 no Outposts. Para fazer uma solicitação com o URL, use o pacote `Requests`.

```
import argparse
import logging
import boto3
from botocore.exceptions import ClientError
import requests

logger = logging.getLogger(__name__)


def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
```

```
    """
    Generate a presigned S3 on Outposts URL that can be used to perform an
 action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds that the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
        logger.info("Got presigned URL: %s", url)
    except ClientError:
        logger.exception(
            "Couldn't get a presigned URL for client method '%s'.",
 client_method)
        raise
    return url


def usage_demo():
    logging.basicConfig(level=logging.INFO, format='%(levelname)s: %(message)s')

    print('-'*88)
    print("Welcome to the Amazon S3 on Outposts presigned URL demo.")
    print('-'*88)

    parser = argparse.ArgumentParser()
    parser.add_argument('accessPointArn', help="The name of the S3 on Outposts
 access point ARN.")
    parser.add_argument(
        'key', help="For a GET operation, the key of the object in S3 on
 Outposts. For a "
                    "PUT operation, the name of a file to upload.")
    parser.add_argument(
        'action', choices=('get', 'put'), help="The action to perform.")
    args = parser.parse_args()

    s3_client = boto3.client('s3')
```

```
    client_action = 'get_object' if args.action == 'get' else 'put_object'
    url = generate_presigned_url(
        s3_client, client_action, {'Bucket': args.accessPointArn, 'Key':
 args.key}, 1000)

    print("Using the Requests package to send a request to the URL.")
    response = None
    if args.action == 'get':
        response = requests.get(url)
    elif args.action == 'put':
        print("Putting data to the URL.")
        try:
            with open(args.key, 'r') as object_file:
                object_text = object_file.read()
            response = requests.put(url, data=object_text)
        except FileNotFoundError:
            print(f"Couldn't find {args.key}. For a PUT operation, the key must
 be the "
                  f"name of a file that exists on your computer.")

    if response is not None:
        print("Got response:")
        print(f"Status: {response.status_code}")
        print(response.text)

    print('-'*88)


if __name__ == '__main__':
    usage_demo()
```

Amazon S3 no Outposts com Amazon EMR no Outposts local

O Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de big data, como Apache Hadoop e Apache Spark, na AWS a fim de processar e analisar grandes volumes de dados. Ao usar essas estruturas e projetos de código aberto relacionados, é possível processar dados para finalidades analíticas e workloads de inteligência de negócios. O Amazon EMR também ajuda a transformar e mover grandes volumes de dados para dentro e para fora de outros datastores e bancos de dados da AWS, além de oferecer suporte ao Amazon S3 no Outposts. Para obter mais informações sobre o Amazon EMR, consulte Amazon EMR no Outposts no Guia de gerenciamento do Amazon EMR.

Para o Amazon S3 no Outposts, o Amazon EMR começou a oferecer suporte ao conector S3A do Apache Hadoop na versão 7.0.0. As versões anteriores do Amazon EMR não oferecem suporte ao S3 no Outposts local e o EMR File System (EMRFS) não é compatível.

Aplicações compatíveis

O Amazon EMR com o Amazon S3 no Outposts é compatível com as seguintes aplicações:

- Hadoop
- Spark
- Hue
- Hive
- Sqoop
- Pig
- Hudi
- Flink

Para obter mais informações, consulte o Guia de versão do Amazon EMR.

Criar e configurar um bucket do Amazon S3 no Outposts

O Amazon EMR usa o AWS SDK para Java com o Amazon S3 no Outposts para armazenar dados de entrada e dados de saída. Seus arquivos de log do Amazon EMR são armazenados em um local regional do Amazon S3 selecionado por você e não são armazenados localmente no Outpost. Para obter mais informações, consulte Logs do Amazon EMR no Guia de gerenciamento do Amazon EMR.

Para estar em conformidade com os requisitos do Amazon S3 e de DNS, os buckets do S3 no Outposts têm restrições e limitações de nomenclatura. Para obter mais informações, consulte Criar um bucket do S3 on Outposts.

Com o Amazon EMR versão 7.0.0 e posterior, você pode usar o Amazon EMR com o S3 no Outposts e o sistema de arquivos S3A.

Pré-requisitos

Permissões do S3 no Outposts: ao criar um perfil de instância do Amazon EMR, esse perfil deve conter o namespace do AWS Identity and Access Management (IAM) para o S3 no Outposts. O S3

no Outposts tem seu próprio namespace: `s3-outposts*`. Para conferir um exemplo de política que usa esse namespace, consulte Configurar o IAM com o S3 on Outposts.

Conector S3A: para configurar um cluster do EMR para acessar dados de um bucket do Amazon S3 no Outposts, você deve usar o conector S3A do Apache Hadoop. Para usar o conector, garanta que todos os URIs do S3 usem o esquema do `s3a`. Caso contrário, você pode configurar a implementação do sistema de arquivos utilizado para o cluster do EMR de modo que os URIs do S3 funcionem com o conector S3A.

Para configurar a implementação do sistema de arquivos de modo que funcione com o conector S3A, use as propriedades de configuração `fs.`*`file_scheme`*`.impl` e `fs.AbstractFileSystem.`*`file_scheme`*`.impl` para o cluster do EMR, em que *`file_scheme`* corresponde ao tipo de URIs do S3 que você tem. Para usar o exemplo a seguir, substitua os *`user input placeholders`* por suas próprias informações. Por exemplo, para alterar a implementação do sistema de arquivos para URIs do S3 que usam o esquema `s3`, especifique as seguintes propriedades de configuração do cluster:

```
[
  {
"Classification": "core-site",
    "Properties": {
    "fs.s3.impl": "org.apache.hadoop.fs.s3a.S3AFileSystem",
    "fs.AbstractFileSystem.s3.impl": "org.apache.hadoop.fs.s3a.S3A"
    }
  }
]
```

Para usar o S3A, defina a propriedade de configuração `fs.`*`file_scheme`*`.impl` como `org.apache.hadoop.fs.s3a.S3AFileSystem` e defina a propriedade `fs.AbstractFileSystem.`*`file_scheme`*`.impl` como `org.apache.hadoop.fs.s3a.S3A`.

Por exemplo, se você estiver acessando o caminho `s3a://`*`bucket`*`/...`, defina a propriedade `fs.s3a.impl` como `org.apache.hadoop.fs.s3a.S3AFileSystem` e defina a propriedade `fs.AbstractFileSystem.s3a.impl` como `org.apache.hadoop.fs.s3a.S3A`.

Conceitos básicos do Amazon EMR com o Amazon S3 no Outposts

Os tópicos a seguir explicam como começar a usar o Amazon EMR com o Amazon S3 no Outposts.

Tópicos

- Criação de uma política de permissões
- Criação e configuração de um cluster
- Visão geral das configurações
- Considerações

Criação de uma política de permissões

Antes de criar um cluster do EMR que use o Amazon S3 on Outposts, é necessário criar uma política do IAM para anexar ao perfil de instância do Amazon EC2 para o cluster. A política deve ter permissões para acessar o nome do recurso da Amazon (ARN) do ponto de acesso do S3 no Outposts. Para obter mais informações sobre como criar políticas do IAM para o S3 no Outposts, consulte Configurar o IAM com o S3 on Outposts.

O exemplo de política a seguir mostra como conceder as permissões necessárias. Após criar a política, anexe-a à função do perfil de instância usada para criar seu cluster do EMR, conforme descrito na seção the section called “Criação e configuração de um cluster”. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
{
"Version":"2012-10-17",
  "Statement": [
        {
  "Effect": "Allow",
            "Resource": "arn:aws:s3-outposts:us-
west-2:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name,
            "Action": [
                "s3-outposts:*"
            ]
        }
    ]

 }
```

Criação e configuração de um cluster

Para criar um cluster que execute o Spark com o S3 no Outposts, conclua as etapas a seguir no console.

Como criar um cluster que execute o Spark com o S3 no Outposts

1. Abra o console do Amazon EMR em https://console.aws.amazon.com/elasticmapreduce/.
2. No painel de navegação à esquerda, escolha Clusters.
3. Selecione Criar cluster.
4. Em Versão do Amazon EMR, escolha emr-7.0.0 ou posterior.
5. Em Pacote de aplicativos, escolha Spark interativo. Selecione todas as outras aplicações compatíveis que você queira incluir no cluster.
6. Para habilitar o Amazon S3 no Outposts, insira suas configurações.

   Exemplo de configuração

   Para usar o exemplo de configuração a seguir, substitua *user input placeholders* por suas próprias informações.

```
[
 {
   "Classification": "core-site",
   "Properties": {
     "fs.s3a.bucket.DOC-EXAMPLE-BUCKET.accesspoint.arn": "arn:aws:s3-outposts:us-
west-2:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name"
     "fs.s3a.committer.name": "magic",
     "fs.s3a.select.enabled": "false"
    }
  },
  {
    "Classification": "hadoop-env",
    "Configurations": [
      {
        "Classification": "export",
        "Properties": {
          "JAVA_HOME": "/usr/lib/jvm/java-11-amazon-corretto.x86_64"
          }
       }
     ],
     "Properties": {}
   },
   {
     "Classification": "spark-env",
     "Configurations": [
```

```
       {
         "Classification": "export",
         "Properties": {
           "JAVA_HOME": "/usr/lib/jvm/java-11-amazon-corretto.x86_64"
         }
       }
      ],
      "Properties": {}
     },
     {
      "Classification": "spark-defaults",
      "Properties": {
        "spark.executorEnv.JAVA_HOME": "/usr/lib/jvm/java-11-amazon-
corretto.x86_64",
        "spark.sql.sources.fastS3PartitionDiscovery.enabled": "false"
      }
     }
  ]
```

7. Na seção Redes, escolha uma nuvem privada virtual (VPC) e uma sub-rede que estejam no seu rack do AWS Outposts. Para obter mais informações sobre o Amazon EMR no Outposts, consulte Clusters do EMR no AWS Outposts no Guia de gerenciamento do Amazon EMR.
8. Na seção Perfil de instância do EC2 para o Amazon EMR, escolha o perfil do IAM que tem a política de permissões que você criou anteriormente anexada.
9. Defina as configurações restantes do cluster e escolha Criar cluster.

Visão geral das configurações

A tabela a seguir descreve as configurações do S3A e os valores a serem especificados para os respectivos parâmetros ao configurar um cluster que usa o S3 no Outposts com o Amazon EMR.

Parâmetro	Valor padrão	Valor necessário para o S3 no Outposts	Explicação
`fs.s3a.aws.credentials.provider`	Se não for especificado, o S3A procurará o S3 no bucket de regiões com o nome de bucket Outposts.	O ARN do ponto de acesso do bucket do S3 no Outposts.	O Amazon S3 on Outposts oferece suporte a pontos de acesso somente de nuvem privada virtual

Parâmetro	Valor padrão	Valor necessário para o S3 no Outposts	Explicação
			(VPC) como o único meio de acessar os buckets do Outposts.
`fs.s3a.committer.name`	`file`	`magic`	O confirmador Magic é o único confirmador compatível com o S3 no Outposts.
`fs.s3a.select.enabled`	`TRUE`	`FALSE`	O S3 Select não é compatível com o Outposts.
`JAVA_HOME`	`/usr/lib/jvm/java-8`	`/usr/lib/jvm/java-11-amazon-corretto.x86_64`	O S3 no Outposts em S3A requer Java versão 11.

A tabela a seguir descreve as configurações do Spark e os valores a serem especificados para os respectivos parâmetros ao configurar um cluster que usa o S3 no Outposts com o Amazon EMR.

Parâmetro	Valor padrão	Valor necessário para o S3 no Outposts	Explicação
`spark.sql.sources.fastS3PartitionDiscovery.enabled`	`TRUE`	`FALSE`	O S3 no Outposts não oferece suporte à partição rápida.
`spark.executorEnv.JAVA_HOME`	`/usr/lib/jvm/java-8`	`/usr/lib/jvm/java-11-amazon-corretto.x86_64`	O S3 no Outposts em S3A requer Java versão 11.

Considerações

Considere os seguintes pontos ao integrar o Amazon EMR a buckets do S3 no Outposts:

- O Amazon S3 no Outposts é compatível com o Amazon EMR 7.0.0 e posterior.
- O conector S3A é necessário para usar o S3 no Outposts com o Amazon EMR. Somente o S3A tem os recursos necessários para interagir com buckets do S3 no Outposts. Para obter informações sobre a configuração do conector S3A, consulte Prerequisites.
- O Amazon S3 no Outposts só oferece suporte à criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) com o Amazon EMR. Para obter mais informações, consulte the section called “Criptografia de dados”.
- O Amazon S3 no Outposts não oferece suporte a gravações com o FileOutputCommitter do S3A. As gravações com o FileOutputCommitter do S3A em buckets do S3 no Outposts resultam no seguinte erro: InvalidStorageClass: a classe de armazenamento especificada não é válida.
- O Amazon S3 no Outposts não é compatível com o Amazon EMR Sem Servidor nem com o Amazon EMR no EKS.
- Os logs do Amazon EMR são armazenados em um local regional do Amazon S3 selecionado por você e não são armazenados localmente no bucket do S3 no Outposts.

Armazenamento em cache de autorização e autenticação

O S3 no Outposts armazena em cache os dados de autenticação e autorização com segurança e localmente nos racks do Outposts. O cache remove idas e voltas à Região da AWS pai para cada solicitação. Isso elimina a variabilidade introduzida pelas idas e voltas da rede. Com o cache de autenticação e autorização no S3 no Outposts, você tem latências consistentes que são independentes da latência da conexão entre o Outposts e a Região da AWS.

Quando você faz uma solicitação de API do S3 no Outposts, os dados de autenticação e autorização são armazenados em cache com segurança. Os dados em cache são então usados para autenticar as solicitações subsequentes da API de objetos do S3. O S3 no Outposts só armazena em cache os dados de autenticação e autorização quando a solicitação é assinada usando o Signature versão 4A (SigV4A). O cache é armazenado localmente no Outposts dentro do serviço S3 no Outposts. Ele é atualizado de forma assíncrona quando você faz uma solicitação de API do S3. O cache é criptografado e nenhuma chave criptográfica de texto simples é armazenada no Outposts.

O cache é válido por até 10 minutos quando o Outpost está conectado àRegião da AWS. Quando você faz uma solicitação de API do S3 no Outposts, ele é atualizado de forma assíncrona para

garantir que as políticas mais recentes sejam usadas. Se o Outpost for desconectado da Região da AWS, o cache será válido por até 12 horas.

Configurar o cache de autorização e autenticação

O S3 no Outposts armazena automaticamente em cache os dados de autenticação e autorização para solicitações assinadas com o algoritmo SigV4A. Consulte mais informações em Assinar solicitações de API da AWS no Guia do usuário do AWS Identity and Access Management. O algoritmo SigV4A está disponível nas versões mais recentes dos SDKs da AWS. É possível obtê-lo por meio de uma dependência em AWS Common Runtime (CRT) libraries.

Você precisa usar a versão mais recente do SDK da AWS e instalar a versão mais recente do CRT. Por exemplo, você pode executar `pip install awscrt` para obter a versão mais recente do CRT com o Boto3.

O S3 no Outposts não armazena em cache os dados de autenticação e autorização para solicitações assinadas com o algoritmo SigV4.

Validar a assinatura do SigV4A

Você pode usar o AWS CloudTrail para validar se as solicitações foram assinadas com o SigV4A. Consulte mais informações sobre a configuração do CloudTrail para o S3 no Outposts em Monitoramento do S3 no Outposts com logs do AWS CloudTrail.

Depois de configurar o CloudTrail, é possível verificar como uma solicitação foi assinada no campo `SignatureVersion` dos logs do CloudTrail. As solicitações que foram assinadas com SigV4A terão um `SignatureVersion` definido como `AWS4-ECDSA-P256-SHA256`. As solicitações que foram assinadas com o SigV4 terão `SignatureVersion` definido como `AWS4-HMAC-SHA256`.

Segurança no S3 on Outposts

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de data centers e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O Modelo de Responsabilidade Compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa os Serviços da AWS na Nuvem AWS. A AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon S3 on Outoposts, consulte Serviços da AWS em escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e normas aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o S3 on Outposts. Os tópicos a seguir mostram como configurar o S3 on Outposts para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros Serviços da AWS que ajudam a monitorar e proteger os recursos do S3 on Outposts.

Tópicos

- Configurar o IAM com o S3 on Outposts
- Criptografia de dados no S3 on Outposts
- AWS PrivateLink para S3 on Outposts
- Chaves de política específicas de autenticação do AWS Signature Version 4 (SigV4)
- Políticas gerenciadas da AWS para o Amazon S3 no Outposts
- Usar perfis vinculados a serviço para o Amazon S3 no Outposts

Configurar o IAM com o S3 on Outposts

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda um administrador a controlar com segurança o acesso aos recursos da AWS. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para utilizar os recursos do Amazon S3 no Outposts. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional. Por padrão, os usuários não têm permissões para recursos e operações do S3 no Outposts. Para conceder permissões de acesso para recursos do S3 no Outposts e operações de API, você pode usar o IAM para criar usuários, grupos ou perfis e anexar permissões.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no Centro de Identidade do AWS IAM:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Além das políticas do IAM baseadas em identidade, o S3 no Outposts é compatível com políticas de bucket e de ponto de acesso. As políticas de bucket e políticas de ponto de acesso são políticas baseadas em recursos que são anexadas ao recurso S3 no Outposts.

- Uma política de bucket é anexada ao bucket e permite ou nega solicitações ao bucket e aos objetos dele com base nos elementos da política.
- Por outro lado, uma política de ponto de acesso é anexada ao ponto de acesso e permite ou nega solicitações ao ponto de acesso.

A política de ponto de acesso funciona com a política de bucket anexada ao bucket do S3 no Outposts. Para que uma aplicação ou um usuário acesse objetos em um bucket do S3 on Outposts por meio de um ponto de acesso do S3 on Outposts, tanto a política de ponto de acesso quanto a política de bucket devem permitir a solicitação.

As restrições que você incluir em uma política de ponto de acesso se aplicam somente a solicitações feitas por meio desse ponto de acesso. Por exemplo, se um ponto de acesso estiver anexado a um bucket, você não poderá usar a política de ponto de acesso para permitir ou negar solicitações feitas diretamente ao bucket. No entanto, as restrições que você aplicar a uma política de bucket podem permitir ou negar solicitações feitas diretamente ao bucket ou por meio do ponto de acesso.

Em uma política do IAM ou em uma política baseada em recursos, você define quais ações do S3 on Outposts serão permitidas ou negadas. As ações do S3 no Outposts correspondem a operações de API específicas do S3 no Outposts. As ações do S3 on Outposts usam o prefixo de namespace `s3-outposts:`. As solicitações feitas à API de controle do S3 on Outposts em uma Região da AWS e as solicitações feitas a endpoints da API de objeto no Outpost são autenticadas usando o IAM e autorizadas de acordo com o prefixo de namespace `s3-outposts:`. Para trabalhar com o S3 on Outposts, configure os usuários do IAM e autorize-os no namespace `s3-outposts:` do IAM.

Para obter mais informações, consulte Ações, recursos e chaves de condição do Amazon S3 no Outposts na Referência de autorização do serviço.

> **Note**
>
> - As listas de controle de acesso (ACLs) não são compatíveis com o S3 on Outposts.
> - Para ajudar a garantir que o proprietário de um bucket não possa ser impedido de acessar ou excluir objetos, o S3 no Outposts usa o proprietário do bucket como proprietário do objeto por padrão.
> - O S3 em Outposts sempre tem o Bloqueio de acesso público do S3 habilitado para ajudar a garantir que os objetos nunca tenham acesso público.

Para obter mais informações sobre como configurar o IAM para o S3 on Outposts, consulte os tópicos a seguir.

Tópicos

- Entidades principais para S3 no Outposts

- ARNs de recurso para S3 no Outposts
- Exemplo de políticas para S3 no Outposts
- Permissões para os endpoints do S3 on Outposts
- Perfis vinculados a serviço para o S3 no Outposts

Entidades principais para S3 no Outposts

Ao criar uma política baseada em recurso para conceder acesso ao seu bucket do S3 no Outposts, você deve usar o elemento `Principal` para especificar a pessoa ou o aplicativo que pode fazer uma solicitação de uma ação ou operação no respectivo recurso. Para políticas do S3 no Outposts, você pode usar uma das seguintes entidades principais:

- Uma Conta da AWS
- Um usuário do IAM
- Um perfil do IAM
- Todas as entidades principais, por meio da especificação de um caractere curinga (*) em uma política que use um elemento `Condition` para limitar o acesso a um intervalo específico de IPs

> **Important**
>
> Não é possível gravar uma política para um bucket do S3 on Outposts que use um caractere curinga (*) no elemento `Principal`, a menos que a política também inclua uma `Condition` que limite o acesso a um intervalo específico de endereços IPs. Essa restrição ajuda a garantir que não haja acesso público ao bucket do S3 on Outposts. Para ver um exemplo, consulte Exemplo de políticas para S3 no Outposts.

Para obter mais informações sobre o elemento `Principal`, consulte Elementos de política JSON da AWS: entidade principal no Guia do usuário do IAM.

ARNs de recurso para S3 no Outposts

Os nomes de recurso da Amazon (ARNs) para o S3 on Outposts contêm o ID do Outpost, bem como a Região da AWS na qual se encontra o Outpost, o ID da Conta da AWS e o nome do recurso. Para acessar e executar ações em buckets e objetos do Outposts, é necessário usar um dos formatos de ARN mostrados na tabela a seguir.

O valor *partition* no ARN refere-se a um grupo de Regiões da AWS. O escopo de cada Conta da AWS é uma partição. Estas são as partições compatíveis:

- `aws` – Regiões da AWS
- `aws-us-gov`: regiões AWS GovCloud (US)

A tabela a seguir mostra os formatos de ARN do S3 no Outposts.

ARN do Amazon S3 no Outposts	Formato ARN	Exemplo
ARN do bucket	arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /bucket/*bucket_name*	arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904* /bucket/*amzn-s3-demo-bucket1*
ARN do ponto de acesso	arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /accesspoint/ *accesspoint_name*	arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904* /accesspoint/ *access-point-name*
ARN do objeto	arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /bucket/*bucket_name* /object/*object_key*	arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904* /bucket/*amzn-s3-demo-bucket1* */object/myobject*

ARN do Amazon S3 no Outposts	Formato ARN	Exemplo
ARN do objeto de ponto de acesso do S3 on Outposts (usado nas políticas)	arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /accesspoint/ *accesspoint_name* /object/*object_key*	arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904* /accesspoint/ *access-point-name/object/myobject*
ARN do S3 no Outposts	arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id*	arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904*

Exemplo de políticas para S3 no Outposts

Example: política de bucket do S3 on Outposts com uma entidade principal da Conta da AWS

A política de bucket a seguir usa uma entidade principal da Conta da AWS para conceder acesso a um bucket do S3 no Outposts. Para usar essa política de bucket, substitua os *user input placeholders* por suas próprias informações.

Example: política de bucket do S3 on Outposts com uma entidade principal de caractere curinga (*) e chave de condição para limitar o acesso a um intervalo específico de endereços IPs

A política de bucket a seguir usa uma entidade principal de caractere curinga (*) com a condição `aws:SourceIp` para limitar o acesso a um intervalo específico de endereços IPs. Para usar essa política de bucket, substitua os *user input placeholders* por suas próprias informações.

Permissões para os endpoints do S3 on Outposts

O S3 on Outposts requer suas próprias permissões no IAM para gerenciar ações de endpoint do S3 on Outposts.

> **Note**
>
> - Para endpoints que usam o tipo de acesso de grupo de endereços IP de propriedade do cliente (grupo de CoIP), você também precisa ter permissões para trabalhar com endereços IP de seu grupo de CoIP, conforme descrito na tabela a seguir.
> - Os usuários em contas compartilhadas que acessam o S3 on Outposts usando o AWS Resource Access Manager não podem criar seus próprios endpoints em uma sub-rede compartilhada. Se o usuário de uma conta compartilhada quiser gerenciar seus próprios endpoints, a conta compartilhada deverá criar sua própria sub-rede no Outpost. Para obter mais informações, consulte the section called “Compartilhar o S3 on Outposts”.

A tabela a seguir mostra as permissões do IAM relacionadas ao endpoint do S3 no Outposts.

Ação	Permissões do IAM

`CreateEndpoint`	`s3-outposts:CreateEndpoint`
	
	`ec2:CreateNetworkInterface`
	
	`ec2:DescribeNetworkInterfaces`
	
	`ec2:DescribeVpcs`
	
	`ec2:DescribeSecurityGroups`
	
	`ec2:DescribeSubnets`
	
	`ec2:CreateTags`
	
	`iam:CreateServiceLinkedRole`
	
	Para endpoints que estão usando o tipo de acesso ao grupo de endereços IP de proprieda de do cliente (grupo do CoIP) on-premises, são necessárias as seguintes permissões adicionai s:
	
	`s3-outposts:CreateEndpoint`

Ação	Permissões do IAM

	`ec2:DescribeCoipPools`
	
	`ec2:GetCoipPoolUsage`
	
	`ec2:AllocateAddress`
	
	`ec2:AssociateAddress`
	
	`ec2:DescribeAddresses`
	
	`ec2:DescribeLocalGatewayRou teTableVpcAssociations`

`DeleteEndpoint`	`s3-outposts:DeleteEndpoint`
	
	`ec2:DeleteNetworkInterface`
	
	`ec2:DescribeNetworkInterfaces`
	
	Para endpoints que estão usando o tipo de acesso ao grupo de endereços IP de proprieda de do cliente (grupo do CoIP) on-premises, são necessárias as seguintes permissões adicionai s:
	
	`s3-outposts:DeleteEndpoint`
	
	`ec2:DisassociateAddress`
	
	`ec2:DescribeAddresses`
	
	`ec2:ReleaseAddress`

`ListEndpoints`	`s3-outposts:ListEndpoints`

> **Note**
>
> Você pode usar tags de recurso em uma política do IAM para gerenciar permissões.

Perfis vinculados a serviço para o S3 no Outposts

O S3 no Outposts usa perfis vinculados a serviço do IAM para criar alguns recursos de rede em seu nome. Para obter mais informações, consulte Usar perfis vinculados a serviço para o Amazon S3 no Outposts.

Criptografia de dados no S3 on Outposts

Por padrão, todos os dados armazenados no Amazon S3 on Outposts são criptografados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Consulte mais informações em Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) no Guia do usuário do Amazon S3.

Você também pode optar por usar a criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C). Para usar o SSE-C, especifique uma chave de criptografia como parte das solicitações da API de objeto. A criptografia no lado do servidor criptografa somente os dados de objeto, não os metadados de objeto. Consulte mais informações em Como usar criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C) no Guia do usuário do Amazon S3.

> **Note**
>
> O S3 on Outposts não é compatível com a criptografia no lado do servidor usando chaves do AWS Key Management Service (AWS KMS) (SSE-KMS).

AWS PrivateLink para S3 on Outposts

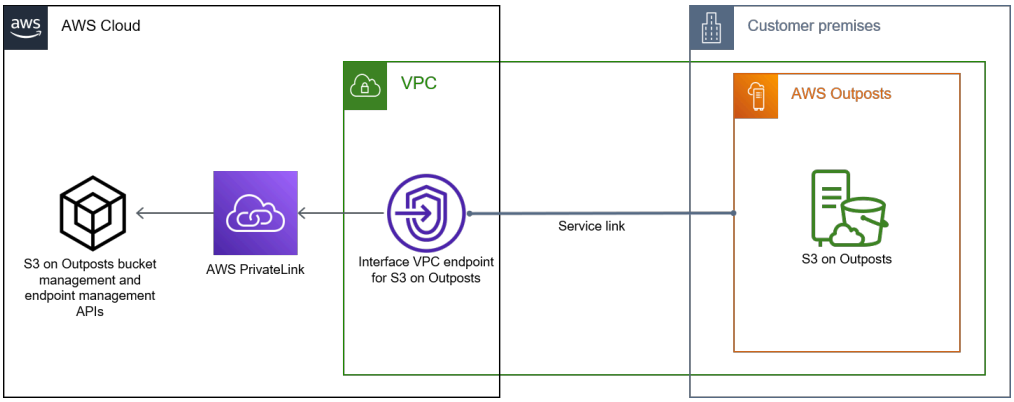
O S3 no Outposts é compatível com o AWS PrivateLink, que fornece acesso direto de gerenciamento ao armazenamento do S3 no Outposts por meio de um endpoint privado na rede privada virtual. Isso permite que você simplifique a arquitetura de rede interna e realize operações de gerenciamento no armazenamento de objetos do Outposts usando endereços IP privados na nuvem privada virtual (VPC). Usar o AWS PrivateLink elimina a necessidade de usar endereços IP públicos ou servidores proxy.

Com o AWS PrivateLink para o Amazon S3 no Outposts, é possível provisionar endpoints da VPC de interface na nuvem privada virtual (VPC) para acessar as APIs de gerenciamento de bucket e gerenciamento de endpoint do S3 no Outposts. Os endpoints da VPC de interface são

diretamente acessíveis por aplicações implantadas na VPC ou no ambiente on-premises por meio da rede privada virtual (VPN) ou do AWS Direct Connect. Você pode acessar as APIs de gerenciamento de buckets e endpoints por meio do AWS PrivateLink. O AWS PrivateLink não é compatível com operações de transferência de dados da API, como GET, PUT e APIs semelhantes. Essas operações já são transferidas de forma privada por meio da configuração do ponto de acesso e do endpoint do S3 no Outposts. Para obter mais informações, consulte Redes para S3 on Outposts.

Os endpoints de interface são representados por uma ou mais interfaces de rede elástica (ENIs) que recebem endereços IP privados de sub-redes em sua VPC. As solicitações realizadas para endpoints de interface para o S3 on Outposts são encaminhadas automaticamente para as APIs de gerenciamento de buckets e endpoints do S3 on Outposts na rede da AWS. Você também pode acessar endpoints de interface em sua VPC via aplicações on-premises por meio do AWS Direct Connect ou da AWS Virtual Private Network (Site-to-Site VPN). Para obter mais informações sobre como conectar sua VPC à rede on-premises, consulte o Guia do usuário do Direct Connect e o Guia do usuário do AWS Site-to-Site VPN.

Os endpoints de interface encaminham as solicitações para APIs de gerenciamento de buckets e endpoints do S3 on Outposts pela rede da AWS e por meio do AWS PrivateLink, conforme ilustrado no diagrama a seguir.



Para obter informações gerais sobre endpoints de interface, consulte Endpoints da VPC de interface (AWS PrivateLink) no Manual do AWS PrivateLink.

Tópicos

- Restrições e limitações
- Acessar endpoints da interface do S3 on Outposts
- Atualizar uma configuração de DNS on-premises
- Criar um endpoint da VPC para o S3 on Outposts

- Criar políticas de bucket e políticas de endpoint da VPC para S3 on Outposts

Restrições e limitações

Quando você acessa as APIs de gerenciamento de buckets e endpoints do S3 on Outposts por meio de AWS PrivateLink, há limitações da VPC. Para obter mais informações, consulte Propriedades e limitações de endpoints de interface e Cotas do AWS PrivateLink no Guia do usuário do AWS PrivateLink.

Além disso, o AWS PrivateLink não oferece compatibilidade com:

- Endpoints do Federal Information Processing Standard (FIPS – Padrões Federais de Processamento de Informações
- APIs de transferência de dados do S3 on Outposts; por exemplo, GET, PUT e operações de API de objetos semelhantes.
- DNS privado

Acessar endpoints da interface do S3 on Outposts

Para acessar APIs de gerenciamento de buckets e endpoints do S3 on Outposts usando o AWS PrivateLink, você deve atualizar as aplicações para usar nomes de DNS específicos de endpoint. Quando você cria um endpoint de interface, o AWS PrivateLink gera dois tipos de nome do S3 on Outposts específicos do endpoint: regional e por zona.

- Nomes de DNS regionais: incluem um ID de endpoint da VPC exclusivo, um identificador de serviço, a Região da AWS e `vpce.amazonaws.com`; por exemplo, *`vpce-1a2b3c4d-5e6f`*`.s3-outposts.us-east-1.vpce.amazonaws.com`.
- Nomes de DNS por zona: incluem um ID de endpoint da VPC exclusivo, a zona de disponibilidade, um identificador de serviço, a Região da AWS e `vpce.amazonaws.com`; por exemplo, *`vpce-1a2b3c4d-5e6f`*`-us-east-1a.s3-outposts.us-east-1.vpce.amazonaws.com`. Você pode usar essa opção se sua arquitetura isola zonas de disponibilidade. Por exemplo, você pode usar nomes DNS por zona para contenção de falhas ou para reduzir os custos da transferência de dados regional.

> **Important**
>
> Os endpoints da interface do S3 no Outposts são resolvidos pelo domínio DNS público. O S3 no Outposts não é compatível com DNS privado. Use o parâmetro `--endpoint-url` para todas as APIs de gerenciamento de buckets e endpoints.

Exemplos da AWS CLI

Use os parâmetros `--region` e `--endpoint-url` para acessar as APIs de gerenciamento de buckets e endpoints por meio de endpoints de interface do S3 on Outposts.

Example: usar o URL do endpoint para listar buckets com a API de controle do S3

No exemplo a seguir, substitua a região *us-east-1*, o URL do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e o ID da conta *111122223333* pelas informações apropriadas.

```
aws s3control list-regional-buckets --region us-east-1 --endpoint-url
 https://vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com --account-
id 111122223333
```

AWSExemplos de SDK

Atualize seus SDKs para a versão mais recente e configure seus clientes para usar um URL de endpoint a fim de acessar a API de controle para endpoints de interface do S3 on Outposts.

SDK for Python (Boto3)

Example: use um URL de endpoint para acessar a API de controle do S3

No exemplo a seguir, substitua a região *us-east-1* e o URL de endpoint da VPC *vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com* por informações apropriadas.

```
control_client = session.client(
service_name='s3control',
region_name='us-east-1',
endpoint_url='https://vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com'
)
```

Para obter mais informações, consulte AWS PrivateLink para Amazon S3 no Guia do desenvolvedor do Boto3.

SDK for Java 2.x

Example: use um URL de endpoint para acessar a API de controle do S3

No exemplo a seguir, substitua o URL do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com* e a região *Region.US_EAST_1* por informações apropriadas.

```
// control client
Region region = Region.US_EAST_1;
s3ControlClient = S3ControlClient.builder().region(region)

 .endpointOverride(URI.create("https://vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com"))
                                  .build()
```

Para obter mais informações, consulte `S3ControlClient` na Referência de APIs do AWS SDK para Java.

Atualizar uma configuração de DNS on-premises

Ao usar nomes de DNS específicos do endpoint para acessar os endpoints de interface para as APIs de gerenciamento de buckets e endpoints do S3 on Outposts, você não precisa atualizar seu resolvedor de DNS on-premises. Você pode resolver o nome de DNS específico do endpoint com o endereço IP privado do endpoint de interface do domínio DNS público do S3 on Outposts.

Criar um endpoint da VPC para o S3 on Outposts

Para criar um endpoint da VPC de interface para S3 em Outposts, consulte Criar um endpoint da VPC no Guia do AWS PrivateLink.

Criar políticas de bucket e políticas de endpoint da VPC para S3 on Outposts

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso ao S3 on Outposts. Você também pode usar a condição `aws:sourceVpce` em políticas de bucket do S3 on Outposts para restringir o acesso a buckets específicos de determinado endpoint da VPC. Com as

políticas de endpoint da VPC, você pode controlar o acesso às APIs de gerenciamento de buckets e endpoints do S3 on Outposts. Com as políticas de bucket, você pode controlar o acesso às APIs de gerenciamento de buckets do S3 on Outposts. No entanto, você não pode gerenciar o acesso a ações de objeto para o S3 on Outposts usando `aws:sourceVpce`.

As políticas de acesso para o S3 on Outposts especificam as seguintes informações:

- A entidade principal do AWS Identity and Access Management (IAM) para a qual as ações são permitidas ou negadas.
- As ações de controle do S3 permitidas ou negadas.
- Os recursos do S3 on Outposts nos quais as ações são permitidas ou negadas.

Os exemplos a seguir mostram políticas que restringem o acesso a um bucket ou a um endpoint. Para obter mais informações sobre conectividade de VPC, consulte Network-to-VPC connectivity options (Opções de conectividade entre rede e VPC) no whitepaper da AWS Amazon Virtual Private Cloud Connectivity Options (Opções de conectividade do Amazon Virtual Private Cloud).

Important

- Ao aplicar as políticas de exemplo para endpoints da VPC descritas nesta seção, talvez você bloqueie o acesso ao bucket acidentalmente. As permissões de bucket que limitam o acesso do bucket às conexões originadas de seu endpoint da VPC podem bloquear todas as conexões ao bucket. Para obter informações sobre como corrigir esse problema, consulte Minha política de bucket tem o ID da VPC ou do endpoint da VPC incorreto. Como corrigir a política para que eu possa acessar o bucket? na Central de conhecimento do Suporte.
- Antes de usar a política de bucket de exemplo a seguir, substitua o ID do endpoint da VPC por um valor apropriado para o caso de uso. Caso contrário, não será possível acessar o bucket.
- Se a política permitir apenas o acesso a um bucket do S3 on Outposts por meio de um endpoint da VPC específico, ela desativará o acesso do console para esse bucket porque as solicitações do console não se originam do endpoint da VPC especificado.

Tópicos

- Exemplo: restringir o acesso a um bucket específico a partir de um endpoint da VPC

- Exemplo: negar acesso usando um endpoint da VPC específico em uma política de bucket do S3 on Outposts

Exemplo: restringir o acesso a um bucket específico a partir de um endpoint da VPC

Você pode criar uma política de endpoint que restrinja o acesso apenas a buckets específicos do S3 on Outposts. A política a seguir restringe o acesso à ação GetBucketPolicy somente ao *example-outpost-bucket*. Para usar essa política, substitua os valores de exemplo por seus próprios valores.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "Policy1415115909151",
    "Statement": [
        {
            "Sid": "Access-to-specific-bucket-only",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3-outposts:GetBucketPolicy",
            "Effect": "Allow",
            "Resource": "arn:aws:s3-outposts:us-east-1:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket"
        }
    ]
}
```

Exemplo: negar acesso usando um endpoint da VPC específico em uma política de bucket do S3 on Outposts

A política de bucket do S3 on Outposts a seguir nega acesso a GetBucketPolicy no bucket do *example-outpost-bucket* por meio do endpoint da VPC *vpce-1a2b3c4d*.

A condição `aws:sourceVpce` especifica o endpoint e não requer um nome do recurso da Amazon (ARN) para o recurso de endpoint da VPC, apenas o ID do endpoint. Para usar essa política, substitua os valores de exemplo por seus próprios valores.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "Policy1415115909152",
    "Statement": [
        {
            "Sid": "Deny-access-to-specific-VPCE",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3-outposts:GetBucketPolicy",
            "Effect": "Deny",
            "Resource": "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpce": "vpce-1a2b3c4d"
                }
            }
        }
    ]
}
```

Chaves de política específicas de autenticação do AWS Signature Version 4 (SigV4)

A tabela a seguir mostra as chaves de condição relacionadas à autenticação com o AWS Signature Version 4 (SigV4) que você pode usar com o Amazon S3 no Outposts. Em uma política de bucket, você pode adicionar essas condições para aplicar um comportamento específico quando as solicitações forem autenticadas usando o Signature Version 4. Para obter exemplos de políticas, consulte Exemplos de política de bucket que usam chaves de condição relacionadas ao Signature Version 4. Consulte mais informações sobre como autenticar solicitações usando o Signature versão 4 em Authenticating requests (AWS Signature Version 4) na Referência de API do Amazon Simple Storage Service

Chaves aplicáveis	Descrição

`s3-outposts:authType`	O S3 no Outposts é compatível com vários métodos de autenticação. Você pode usar essa chave de condição opcional para restringir as solicitações recebidas a usar um método específico de autenticação. Por exemplo, é possível usar essa chave de condição para permitir que somente o cabeçalho HTTP `Authorization` seja usado na autenticação de solicitação.
	
	Valores válidos:
	
	`REST-HEADER`
	
	`REST-QUERY-STRING`

`s3-outposts:signatureAge`	A duração em milissegundos da validade de uma assinatura em uma solicitação autenticada. Essa condição funciona somente para URLs pré-assinados. No Signature Version 4, a chave de assinatura é válida por até 7 dias. Portanto, as assinaturas também são válidas por até 7 dias. Para obter mais informações, consulte Introduction to signing requests (Introdução à assinatura de solicitações) na Referência de API do Amazon Simple Storage Service. Você pode usar essa condição para limitar ainda mais a idade da assinatura. Exemplo de valor: `600000`
`s3-outposts:x-amz-content-sha256`	É possível usar essa chave de condição para proibir conteúdo não assinado em seu bucket. Ao usar o Signature Version 4, para solicitações que usem o cabeçalho `Authorization`, você adiciona o cabeçalho `x-amz-content-sha256` no cálculo da assinatura e, em seguida, defina seu valor para a carga útil do hash.

Chaves aplicáveis	Descrição
	Você pode usar essa chave de condição em sua política de bucket para negar qualquer upload cujas cargas úteis não estejam assinadas. Por exemplo: • Negar uploads que usem o cabeçalho `Authorization` para autenticar solicitações mas não assinem a carga útil. Para obter mais informações, consulte Transferring payload in a single chunk (Transferência de carga útil em um único bloco) na Referência de API do Amazon Simple Storage Service. • Negar uploads que usem URLs pré-assinados. Os URLs pré-assinados sempre têm um `UNSIGNED_PAYLOAD`. Para obter mais informações, consulte Authenticating requests (Autenticação de solicitações) e Authentication methods (Métodos de autenticação) na Referência de API do Amazon Simple Storage Service. Valor válido: `UNSIGNED-PAYLOAD`

Exemplos de política de bucket que usam chaves de condição relacionadas ao Signature Version 4

Para usar os exemplos a seguir, substitua *`user input placeholders`* por suas próprias informações.

Example: s3-outposts:signatureAge

A política de bucket a seguir nega qualquer solicitação de URL pré-assinado do S3 no Outposts em objetos em `example-outpost-bucket` se a assinatura tiver mais de 10 minutos de idade.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "Deny a presigned URL request if the signature is more than 10
 minutes old",
            "Effect": "Deny",
            "Principal": {"AWS":"444455556666"},
            "Action": "s3-outposts:*",
            "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
            "Condition": {
                "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
                "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
            }
        }
    ]
}
```

Example: s3-outposts:authType

A política de bucket a seguir permite somente solicitações que usem o cabeçalho `Authorization` para autenticação de solicitação. Todas as solicitações de URL pré-assinado serão negadas, pois os URLs pré-assinados usam parâmetros de consulta para fornecer informações de solicitação e autenticação. Para obter mais informações, consulte Authentication methods (Métodos de autenticação) na Referência de API do Amazon Simple Storage Service.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
         {
               "Sid": "Allow only requests that use the Authorization header for
 request authentication. Deny presigned URL requests.",
               "Effect": "Deny",
               "Principal": {"AWS":"111122223333"},
               "Action": "s3-outposts:*",
               "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
               "Condition": {
                     "StringNotEquals": {
                           "s3-outposts:authType": "REST-HEADER"
```

```
                }
            }
        }
    ]
}
```

Example: s3-outposts:x-amz-content-sha256

A política de bucket a seguir nega qualquer upload com cargas úteis não assinadas, como uploads que estejam usando URLs pré-assinados. Para obter mais informações, consulte Authenticating requests (Autenticação de solicitações) e Authentication methods (Métodos de autenticação) na Referência de API do Amazon Simple Storage Service.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
         {
               "Sid": "Deny uploads with unsigned payloads.",
               "Effect": "Deny",
               "Principal": {"AWS":"111122223333"},
               "Action": "s3-outposts:*",
               "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
               "Condition": {
                     "StringEquals": {
                           "s3-outposts:x-amz-content-sha256": "UNSIGNED-PAYLOAD"
                     }
               }
         }
   ]
}
```

Políticas gerenciadas da AWS para o Amazon S3 no Outposts

Uma política gerenciada pela AWS é uma política autônoma criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns e permitir a atribuição de permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para casos de uso específicos, por estarem disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Não é possível alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada por AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política estiver vinculada. É provável que a AWS atualize uma política gerenciada por AWS quando um novo AWS service (Serviço da AWS) for lançado, ou novas operações de API forem disponibilizadas para os serviços existentes.

Para saber mais, consulte AWSPolíticas gerenciadas pela no Guia do usuário do IAM.

Política gerenciada da AWS: AWSS3OnOutpostsServiceRolePolicy

Ajuda a gerenciar recursos de rede para você como parte do perfil vinculado a serviço `AWSServiceRoleForS3OnOutposts`.

Para visualizar as permissões dessa política, consulte AWSS3OnOutpostsServiceRolePolicy.

Atualizações do S3 no Outposts em políticas gerenciadas da AWS

Visualize detalhes sobre atualizações em políticas gerenciadas da AWS do S3 no Outposts desde o momento em que esse serviço começou a monitorar essas alterações.

Alteração	Descrição	Data
O S3 no Outposts adicionou `AWSS3OnOutpostsServiceRolePolicy`	O S3 no Outposts adicionou `AWSS3OnOutpostsServiceRolePolicy` como parte do perfil vinculado a serviço `AWSServic`	3 de outubro de 2023

Alteração	Descrição	Data
	`eRoleForS3OnOutpos ts` , que ajuda a gerenciar os recursos de rede para você.	
O S3 no Outposts começou a monitorar alterações	O S3 no Outposts começou a monitorar alterações nas políticas gerenciadas da AWS.	3 de outubro de 2023

Usar perfis vinculados a serviço para o Amazon S3 no Outposts

O Amazon S3 no Outposts usa perfis vinculados a serviço do AWS Identity and Access Management (IAM). O perfil vinculado a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao S3 no Outposts. Os perfis vinculados a serviço são predefinidos pelo S3 no Outposts e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Um perfil vinculado a serviço facilita a configuração do S3 no Outposts porque você não precisa adicionar as permissões necessárias manualmente. O S3 no Outposts define as permissões dos perfis vinculados a serviço. Além disso, exceto se definido de outra forma, somente o S3 no Outposts pode assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege os recursos do S3 no Outposts, pois não é possível remover por engano a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados aos serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de perfil vinculado a serviço para o S3 no Outposts

O S3 no Outposts usa o perfil vinculado a serviço denominado AWSServiceRoleForS3OnOutposts para ajudar a gerenciar recursos de rede para você.

O perfil vinculado ao serviço `AWSServiceRoleForS3OnOutposts` confia nos seguintes serviços para aceitar o perfil:

- `s3-outposts.amazonaws.com`

A política de permissões do perfil denominada `AWSS3OnOutpostsServiceRolePolicy` permite que o S3 no Outposts conclua as seguintes ações nos recursos especificados:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:DescribeCoipPools",
                "ec2:GetCoipPoolUsage",
                "ec2:DescribeAddresses",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
            ],
            "Resource": "*",
            "Sid": "DescribeVpcResources"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Sid": "CreateNetworkInterface"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/CreatedBy": "S3 On Outposts"
                }
            },
            "Sid": "CreateTagsForCreateNetworkInterface"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:ipv4pool-ec2/*"
            ],
            "Sid": "AllocateIpAddress"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:elastic-ip/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/CreatedBy": "S3 On Outposts"
                }
            },
            "Sid": "CreateTagsForAllocateIpAddress"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DisassociateAddress",
                "ec2:ReleaseAddress",
                "ec2:AssociateAddress"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/CreatedBy": "S3 On Outposts"
                }
            },
            "Sid": "ReleaseVpcResources"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateNetworkInterface",
                        "AllocateAddress"
                    ],
                    "aws:RequestTag/CreatedBy": [
                        "S3 On Outposts"
                    ]
                }
            },
            "Sid": "CreateTags"
        }
    ]
}
```

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um perfil) crie, edite ou exclua um perfil vinculado a serviço. Para ter mais informações, consulte Service-linked role permissions (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Criar um perfil vinculado a serviço para o S3 no Outposts

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um endpoint do S3 no Outposts no Console de gerenciamento da AWS, a AWS CLI ou a API da AWS, o S3 no Outposts cria o perfil vinculado a serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria um endpoint do S3 no Outposts, o S3 no Outposts cria o perfil vinculado a serviço para você novamente.

Também é possível usar o console do IAM para criar um perfil vinculado a serviço com o caso de uso do S3 no Outposts. Na AWS CLI ou na API do AWS, crie um perfil vinculado a serviço com o nome de serviço `s3-outposts.amazonaws.com`. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editar um perfil vinculado a serviço para o S3 no Outposts

O S3 no Outposts não permite editar o perfil vinculado a serviço `AWSServiceRoleForS3OnOutposts`. Isso inclui o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir um perfil vinculado a serviço para o S3 no Outposts

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de seu perfil vinculado ao serviço antes de excluí-lo manualmente.

> **Note**
>
> Se o serviço do S3 no Outposts estiver usando o perfil quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir recursos do S3 no Outposts usados pelo perfil AWSServiceRoleForS3OnOutposts

1. Exclua os endpoints do S3 no Outposts na Conta da AWS em todas as Regiões da AWS.
2. Exclua o perfil vinculado a serviço usando o IAM.

   Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada ao serviço `AWSServiceRoleForS3OnOutposts`. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões compatíveis com perfis vinculados a serviço do S3 no Outposts

O S3 no Outposts aceita o uso de perfis vinculados a serviço em todas as Regiões da AWS em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints do S3 no Outposts.

Gerenciar o armazenamento do S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (OUTPOSTS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte . O que é o Amazon S3 on Outposts?

Para obter mais informações sobre como gerenciar e compartilhar sua capacidade de armazenamento do Amazon S3 on Outposts, consulte os tópicos a seguir.

Tópicos

- Gerenciar o versionamento do S3 para um bucket do S3 no Outposts
- Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts
- Replicar objetos para o S3 no Outposts
- Compartilhar o S3 on Outposts usando o AWS RAM
- Outros Serviços da AWS que usam o S3 on Outposts

Gerenciar o versionamento do S3 para um bucket do S3 no Outposts

Quando habilitado, o versionamento do S3 salva várias cópias distintas de um objeto no mesmo bucket. O versionamento do S3 pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado em buckets do Outposts. O versionamento do S3 ajuda você a se recuperar de ações não intencionais de usuários e de falhas da aplicação.

Os buckets do Amazon S3 no Outposts têm três estados de versionamento:

- Unversioned (Sem versionamento): se você nunca habilitou ou suspendeu o versionamento do S3 em seu bucket, ele não tem versionamento e não retorna nenhum status de versionamento do S3.

Para obter mais informações sobre o S3 Versioning, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.

- Enabled (Habilitado): habilita o versionamento do S3 para os objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. Os objetos que já existiam no bucket no momento em que você habilita o controle de versão têm um ID de versão `null`. Se você modificar esses (ou quaisquer outros) objetos com outras operações, como PutObject, os novos objetos receberão um ID de versão exclusivo.
- Suspended (Suspenso): suspende o versionamento do S3 para os objetos no bucket. Todos os objetos adicionados ao bucket depois que o versionamento é suspenso recebem o ID de versão `null`. Consulte mais informações em Adicionar objetos a buckets com versionamento suspenso no Guia do usuário do Amazon S3.

Depois que você habilita o versionamento do S3 para um bucket do S3 no Outposts, ele nunca pode voltar a um estado sem versionamento. No entanto, você pode suspender o versionamento. Para obter mais informações sobre o S3 Versioning, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.

Para cada objeto em um bucket, há uma versão atual e zero ou mais versões desatualizadas. Para reduzir os custos de armazenamento, você pode configurar regras de ciclo de vida do bucket do S3 para expirar as versões desatualizadas após um período especificado. Para obter mais informações, consulte Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts.

Os exemplos a seguir mostram como habilitar ou suspender o versionamento para um bucket do S3 no Outposts usando o Console de gerenciamento da AWS e a AWS Command Line Interface (AWS CLI). Para criar um bucket com versionamento do S3 habilitado, consulte Criar um bucket do S3 on Outposts.

> **Note**
>
> A Conta da AWS que cria o bucket é proprietária dele e é a única que pode confirmar suas ações. Os buckets têm propriedades de configuração como Outpost, etiquetas, criptografia padrão e configurações de ponto de acesso. As configurações de ponto de acesso incluem a nuvem privada virtual (VPC), a política do ponto de acesso para acessar os objetos no bucket e outros metadados. Para obter mais informações, consulte Especificações do Amazon S3 no Outposts.

Usar o console do S3

Como editar as configurações de versionamento do S3 para um bucket

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts para o qual você deseja habilitar o versionamento do S3.
4. Escolha a guia Properties (Propriedades).
5. Em Bucket Versioning (Versionamento de bucket), escolha Edit (Editar).
6. Edite as configurações de versionamento do S3 para o bucket escolhendo uma das seguintes opções:
   - Para suspender o versionamento do S3 e interromper a criação de versões de objetos, escolha Suspend (Suspender).
   - Para habilitar o versionamento do S3 e salvar várias cópias distintas de cada objeto, escolha Enable (Habilitar).
7. Escolha Salvar alterações.

Como usar o AWS CLI

Para habilitar ou suspender o versionamento do S3 para um bucket usando a AWS CLI, use o comando `put-bucket-versioning` conforme mostrado nos exemplos a seguir. Para usar esses exemplos, substitua cada *`user input placeholder`* por suas próprias informações.

Para obter mais informações, consulte put-bucket-versioning na Referência da AWS CLI.

Example: Habilitar o versionamento do S3

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket --versioning-configuration Status=Enabled
```

Example: Suspender o versionamento do S3

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket --versioning-configuration Status=Suspended
```

Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts

Você pode usar o Ciclo de Vida do S3 para otimizar a capacidade de armazenamento do Amazon S3 no Outposts. Você pode criar regras de ciclo de vida para expirar objetos à medida que envelhecem ou quando são substituídos por versões mais recentes. Você pode criar, habilitar, desabilitar e excluir uma regra de ciclo de vida.

Para obter mais informações sobre o ciclo de vida do S3, consulte Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts.

> **Note**
>
> A Conta da AWS que cria o bucket tem propriedade sobre ele e é a única que pode criar, habilitar, desabilitar e excluir uma regra de ciclo de vida.

Para criar e gerenciar a configuração do ciclo de vida do bucket do S3 on Outposts, consulte os tópicos a seguir.

Tópicos

- Criar e gerenciar uma regra de ciclo de vida usando o Console de gerenciamento da AWS
- Criar e gerenciar uma configuração de ciclo de vida usando a AWS CLI e o SDK para Java

Criar e gerenciar uma regra de ciclo de vida usando o Console de gerenciamento da AWS

Você pode usar o Ciclo de Vida do S3 para otimizar a capacidade de armazenamento do Amazon S3 no Outposts. Você pode criar regras de ciclo de vida para expirar objetos à medida que envelhecem ou quando são substituídos por versões mais recentes. Você pode criar, habilitar, desabilitar e excluir uma regra de ciclo de vida.

Para obter mais informações sobre o ciclo de vida do S3, consulte Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts.

> **Note**
>
> A Conta da AWS que cria o bucket tem propriedade sobre ele e é a única que pode criar, habilitar, desabilitar e excluir uma regra de ciclo de vida.

Para criar e gerenciar uma regra de ciclo de vida para um S3 no Outposts usando o Console de gerenciamento da AWS, consulte os tópicos a seguir.

Tópicos

- Criar uma regra de ciclo de vida
- Habilitar uma regra de ciclo de vida
- Editar uma regra de ciclo de vida
- Excluir uma regra de ciclo de vida

Criar uma regra de ciclo de vida

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts para o qual você deseja criar uma regra de ciclo de vida.
4. Escolha a guia Management (Gerenciamento) e escolha Create Lifecycle rule (Criar regra de ciclo de vida).
5. Insira um valor para Lifecycle rule name (Nome da regra do ciclo de vida).
6. Em Rule scope (Escopo da regra), escolha uma das seguintes opções:
   - Para limitar o escopo a filtros específicos, escolha Limit the scope of this rule using one or more filters (Limitar o escopo desta regra usando um ou mais filtros). Depois, adicione um filtro de prefixos, etiquetas ou tamanho de objeto.
   - Para aplicar a regra a todos os objetos no bucket, escolha Apply to all objects in the bucket (Aplicar a todos os objetos no bucket).
7. Em Lifecycle rule actions (Ações de regra de ciclo de vida), escolha uma das seguintes opções:
   - Expire current versions of objects (Expirar versões atuais de objetos): para buckets com versionamento habilitado, o S3 no Outposts adiciona um marcador de exclusão e retém os

objetos como versões não atuais. Para buckets que não usam o versionamento do S3, o S3 no Outposts exclui permanentemente os objetos.

- Permanently delete noncurrent versions of objects (Excluir permanentemente versões de objetos desatualizadas): o S3 no Outposts exclui permanentemente as versões de objetos desatualizadas.
- Delete expired object delete markers or incomplete multipart uploads (Excluir marcadores de exclusão de objetos expirados ou multipart uploads incompletos): o S3 no Outposts exclui permanentemente marcadores de exclusão de objetos expirados ou multipart uploads incompletos.

  Se você limitar o escopo da sua regra de ciclo de vida usando etiquetas de objeto, não poderá escolher a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados). Também não poderá escolher a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados) se escolher a opção Expire current object versions (Expirar as versões atuais do objeto).

> **Note**
>
> Filtros baseados em tamanho não podem ser usados com marcadores de exclusão e multipart uploads incompletos.

8. Se você escolheu a opção Expire current versions of objects (Expirar versões atuais de objetos) ou Permanently delete noncurrent versions of objects (Excluir permanentemente versões não atuais de objetos), configure o gatilho de regra com base em uma data específica ou com base na idade do objeto.
9. Se você escolheu a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados), para confirmar que deseja excluir os marcadores de exclusão de objetos expirados, selecione a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados).
10. Em Timeline Summary (Resumo da linha do tempo), revise sua regra de ciclo de vida e escolha Create rule (Criar regra).

Habilitar uma regra de ciclo de vida

Para habilitar e desabilitar uma regra de ciclo de vida de bucket

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts para o qual deseja habilitar e desabilitar uma regra de ciclo de vida.
4. Escolha a guia Management (Gerenciamento) e, em Lifecycle rule (Regra de ciclo de vida), selecione a regra que deseja habilitar ou desabilitar.
5. Em Action (Ação), escolha Enable or disable rule (Habilitar e desabilitar regra).

Editar uma regra de ciclo de vida

1. Abra o console do Amazon S3, em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts para o qual você deseja editar uma regra de ciclo de vida.
4. Escolha a guia Management (Gerenciamento) e escolha a Lifecycle rule (Regra de ciclo de vida) que você deseja editar.
5. (Opcional) Atualize o valor de Lifecycle rule name (Nome da regra de ciclo de vida).
6. Em Rule scope (Escopo da regra), edite o escopo conforme necessário:
   - Para limitar o escopo a filtros específicos, escolha Limit the scope of this rule using one or more filters (Limitar o escopo desta regra usando um ou mais filtros). Depois, adicione um filtro de prefixos, etiquetas ou tamanho de objeto.
   - Para aplicar a regra a todos os objetos no bucket, escolha Apply to all objects in the bucket (Aplicar a todos os objetos no bucket).
7. Em Lifecycle rule actions (Ações de regra de ciclo de vida), escolha uma das seguintes opções:
   - Expire current versions of objects (Expirar versões atuais de objetos): para buckets com versionamento habilitado, o S3 no Outposts adiciona um marcador de exclusão e retém os objetos como versões não atuais. Para buckets que não usam o versionamento do S3, o S3 no Outposts exclui permanentemente os objetos.

- Permanently delete noncurrent versions of objects (Excluir permanentemente versões de objetos desatualizadas): o S3 no Outposts exclui permanentemente as versões de objetos desatualizadas.
- Delete expired object delete markers or incomplete multipart uploads (Excluir marcadores de exclusão de objetos expirados ou multipart uploads incompletos): o S3 no Outposts exclui permanentemente marcadores de exclusão de objetos expirados ou multipart uploads incompletos.

  Se você limitar o escopo da sua regra de ciclo de vida usando etiquetas de objeto, não poderá escolher a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados). Também não poderá escolher a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados) se escolher a opção Expire current object versions (Expirar as versões atuais do objeto).

> **Note**
>
> Filtros baseados em tamanho não podem ser usados com marcadores de exclusão e multipart uploads incompletos.

8. Se você escolheu a opção Expire current versions of objects (Expirar versões atuais de objetos) ou Permanently delete noncurrent versions of objects (Excluir permanentemente versões não atuais de objetos), configure o gatilho de regra com base em uma data específica ou com base na idade do objeto.
9. Se você escolheu a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados), para confirmar que deseja excluir os marcadores de exclusão de objetos expirados, selecione a opção Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados).
10. Selecione Salvar.

Excluir uma regra de ciclo de vida

1. Abra o console do Amazon S3, em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o bucket do Outposts para o qual você deseja excluir uma regra de ciclo de vida.

4. Escolha a guia Management (Gerenciamento) e, em Lifecycle rule (Regra de ciclo de vida), selecione a regra que deseja excluir.
5. Escolha Excluir.

Criar e gerenciar uma configuração de ciclo de vida usando a AWS CLI e o SDK para Java

Você pode usar o Ciclo de Vida do S3 para otimizar a capacidade de armazenamento do Amazon S3 no Outposts. Você pode criar regras de ciclo de vida para expirar objetos à medida que envelhecem ou quando são substituídos por versões mais recentes. Você pode criar, habilitar, desabilitar e excluir uma regra de ciclo de vida.

Para obter mais informações sobre o ciclo de vida do S3, consulte Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts.

> **Note**
>
> A Conta da AWS que cria o bucket tem propriedade sobre ele e é a única que pode criar, habilitar, desabilitar e excluir uma regra de ciclo de vida.

Para criar e gerenciar uma configuração de ciclo de vida de um bucket do S3 on Outposts usando a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java, consulte os exemplos a seguir.

Tópicos

- Executar PUT em uma configuração de ciclo de vida
- Executar GET na configuração de ciclo de vida em um bucket do S3 on Outposts

Executar PUT em uma configuração de ciclo de vida

AWS CLI

O exemplo a seguir da AWS CLI coloca uma política de configuração de ciclo de vida em um bucket do Outposts. Essa política especifica que todos os objetos que têm o prefixo sinalizado (*`myprefix`*) e tags expiram após dez dias. Para usar esse exemplo, substitua cada *`user input placeholder`* por suas próprias informações.

1. Salve a política da configuração do ciclo de vida em um arquivo JSON. Neste exemplo, o nome do arquivo é `lifecycle1.json`.

```
{
    "Rules": [
        {
            "ID": "id-1",
            "Filter": {
                "And": {
                    "Prefix": "myprefix",
                    "Tags": [
                        {
                            "Value": "mytagvalue1",
                            "Key": "mytagkey1"
                        },
                        {
                            "Value": "mytagvalue2",
                            "Key": "mytagkey2"
                        }
                    ],
                    "ObjectSizeGreaterThan": 1000,
                    "ObjectSizeLessThan": 5000
                }
            },
            "Status": "Enabled",
            "Expiration": {
                "Days": 10
            }
        }
    ]
}
```

2. Envie o arquivo JSON como parte do comando `put-bucket-lifecycle-configuration` da CLI. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte put-bucket-lifecycle-configuration na Referência da AWS CLI.

```
aws s3control put-bucket-lifecycle-configuration --account-id 123456789012 --
bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/
bucket/example-outposts-bucket --lifecycle-configuration file://lifecycle1.json
```

SDK for Java

O exemplo a seguir do SDK para Java coloca uma configuração de ciclo de vida em um bucket do Outposts. Essa configuração de ciclo de vida especifica que todos os objetos que têm o prefixo sinalizado (*myprefix*) e tags expiram após dez dias. Para usar esse exemplo, substitua cada *user input placeholder* por suas próprias informações. Para obter mais informações, consulte PutBucketLifecycleConfiguration na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void putBucketLifecycleConfiguration(String bucketArn) {

    S3Tag tag1 = new S3Tag().withKey("mytagkey1").withValue("mytagkey1");
    S3Tag tag2 = new S3Tag().withKey("mytagkey2").withValue("mytagkey2");

    LifecycleRuleFilter lifecycleRuleFilter = new LifecycleRuleFilter()
            .withAnd(new LifecycleRuleAndOperator()
                    .withPrefix("myprefix")
                    .withTags(tag1, tag2))
                    .withObjectSizeGreaterThan(1000)
                    .withObjectSizeLessThan(5000);

    LifecycleExpiration lifecycleExpiration = new LifecycleExpiration()
            .withExpiredObjectDeleteMarker(false)
            .withDays(10);

    LifecycleRule lifecycleRule = new LifecycleRule()
            .withStatus("Enabled")
            .withFilter(lifecycleRuleFilter)
            .withExpiration(lifecycleExpiration)
            .withID("id-1");

    LifecycleConfiguration lifecycleConfiguration = new LifecycleConfiguration()
            .withRules(lifecycleRule);

    PutBucketLifecycleConfigurationRequest reqPutBucketLifecycle = new
 PutBucketLifecycleConfigurationRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn)
            .withLifecycleConfiguration(lifecycleConfiguration);
```

```
    PutBucketLifecycleConfigurationResult respPutBucketLifecycle =
 s3ControlClient.putBucketLifecycleConfiguration(reqPutBucketLifecycle);
    System.out.printf("PutBucketLifecycleConfiguration Response: %s%n",
 respPutBucketLifecycle.toString());

}
```

Executar GET na configuração de ciclo de vida em um bucket do S3 on Outposts

AWS CLI

O seguinte exemplo da AWS CLI obtém uma configuração de ciclo de vida em um bucket do Outposts. Para usar esse comando, substitua cada *`user input placeholder`* por suas próprias informações. Para obter mais informações sobre esse comando, consulte get-bucket-lifecycle-configuration na Referência da AWS CLI.

```
aws s3control get-bucket-lifecycle-configuration --account-id 123456789012 --bucket
 arn:aws:s3-outposts:<your-region>:123456789012:outpost/op-01ac5d28a6a232904/
bucket/example-outposts-bucket
```

SDK for Java

O exemplo a seguir do SDK para Java obtém uma configuração de ciclo de vida de um bucket do Outposts. Para obter mais informações, consulte GetBucketLifecycleConfiguration na Referência da API do Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void getBucketLifecycleConfiguration(String bucketArn) {

    GetBucketLifecycleConfigurationRequest reqGetBucketLifecycle = new
 GetBucketLifecycleConfigurationRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn);

    GetBucketLifecycleConfigurationResult respGetBucketLifecycle =
 s3ControlClient.getBucketLifecycleConfiguration(reqGetBucketLifecycle);
    System.out.printf("GetBucketLifecycleConfiguration Response: %s%n",
 respGetBucketLifecycle.toString());

}
```

Replicar objetos para o S3 no Outposts

Com a replicação do S3 no AWS Outposts, você pode configurar o Amazon S3 no Outposts para replicar automaticamente objetos do S3 em diferentes Outposts ou entre buckets no mesmo Outpost. Você pode usar a replicação do S3 no Outposts para manter várias réplicas dos dados no mesmo ou em diferentes Outposts, ou em contas diferentes, para ajudar a atender às necessidades de residência de dados. A replicação do S3 no Outposts ajuda a atender às suas necessidades de armazenamento compatíveis e ao compartilhamento de dados entre contas. Se você precisa garantir que as réplicas sejam idênticas aos dados de origem, poderá usar a replicação do S3 no Outposts para fazer réplicas dos objetos que retêm todos os metadados, como o tempo de criação do objeto original, as tags e os IDs de versão.

A replicação do S3 no Outposts também fornece métricas e notificações detalhadas para monitorar o status da replicação de objetos entre buckets. Você pode usar o Amazon CloudWatch para monitorar o andamento da replicação rastreando bytes pendentes de replicação, operações pendentes de replicação e latência de replicação entre os buckets de origem e destino. Para diagnosticar e corrigir rapidamente os problemas de configuração, você também pode configurar o Amazon EventBridge para receber notificações sobre falhas de objetos de replicação. Para saber mais, consulte Gerenciar sua replicação.

Tópicos

- Configuração de replicação
- Requisitos para a replicação do S3 no Outposts
- O que é replicado?
- O que não é replicado?
- O que não é compatível com a replicação do S3 no Outposts?
- Configuração da replicação
- Gerenciar sua replicação

Configuração de replicação

O S3 no Outposts armazena uma configuração de replicação como XML. No arquivo XML de configuração da replicação, você especifica uma função do AWS Identity and Access Management (IAM) e uma ou mais regras.

```
<ReplicationConfiguration>
```

```
    <Role>IAM-role-ARN</Role>
    <Rule>
        ...
    </Rule>
    <Rule>
         ...
    </Rule>
     ...
</ReplicationConfiguration>
```

O S3 no Outposts não pode replicar objetos sem sua permissão. Você concede permissões do S3 no Outposts com o perfil do IAM especificada na configuração de replicação. O S3 no Outposts assume esse perfil do IAM para replicar objetos em seu nome. Você precisa conceder as permissões necessárias ao perfil do IAM antes de iniciar a replicação. Para obter mais informações sobre essas permissões para Outposts S3 no Outposts, consulte Criar uma função do IAM.

Você adiciona uma regra na configuração da replicação nos seguintes cenários:

- Você quer replicar todos os objetos.
- Você quer replicar um subgrupo de objetos. Você identifica o subgrupo do objeto adicionando um filtro à regra. No filtro, você especifica um prefixo de chaves do objeto, tags ou uma combinação de ambos, de maneira a identificar o subgrupo de objetos aos quais a regra se aplica.

Você adicionará várias regras a uma configuração de replicação, se desejar selecionar um subgrupo diferente de objetos. Em cada regra, você especifica um filtro que seleciona um subgrupo diferente de objetos. Por exemplo, talvez você queira replicar objetos com os prefixos de chaves `tax/` ou `document/`. Para fazer isso, você adiciona duas regras, uma que especifica o filtro de prefixo das chaves `tax/` e outro que especifica o prefixo das chaves `document/`.

Para obter mais informações sobre a configuração de replicação e as regras de replicação do S3 no Outposts, consulte ReplicationConfiguration na Referência de API do Amazon Simple Storage Service.

Requisitos para a replicação do S3 no Outposts

A replicação exige o seguinte:

- O intervalo CIDR do Outpost de destino deve estar associado à tabela de sub-rede do Outpost de origem. Para obter mais informações, consulte Pré-requisitos para criar regras de replicação.

- Tanto o bucket de origem quanto o de destino devem ter o versionamento do S3 ativado. Para obter mais informações sobre versionamento, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.
- O Amazon S3 no Outposts deve ter permissão para replicar objetos do bucket de origem para o bucket de destino em seu nome. Isso significa que você deve criar um perfil de serviço para delegar as permissões `GET` e `PUT` ao S3 no Outposts.
  1. Antes de criar o perfil de serviço, você deve ter a permissão `GET` no bucket de origem e a permissão `PUT` no bucket de destino.
  2. Para criar o perfil de serviço para delegar permissões ao S3 no Outposts, você deve primeiro configurar as permissões para permitir que uma entidade do IAM (um usuário ou perfil) execute as ações `iam:CreateRole` e `iam:PassRole`. Depois, permita que a entidade do IAM crie um perfil de serviço. Para fazer com que o S3 no Outposts assuma o perfil de serviço em seu nome e delegue as permissões `GET` e `PUT` ao S3 no Outposts, você deve atribuir as políticas de permissões e confiança necessárias ao perfil. Para obter mais informações sobre essas permissões para Outposts S3 no Outposts, consulte Criar uma função do IAM. Para obter mais informações sobre como criar um perfil de serviço, consulte Criar um perfil de serviço.

O que é replicado?

Por padrão, o S3 no Outposts replica o seguinte:

- Objetos criados depois de adicionar uma configuração de replicação.
- Metadados de objeto dos objetos de origem para as réplicas. Para obter informações sobre como replicar metadados das réplicas para os objetos de origem, consulte Status da replicação se a sincronização de modificação de réplica do Amazon S3 no Outposts estiver ativada.
- Tags de objeto, se houver.

Como a exclusão de operações afeta a replicação

Se você excluir um objeto do bucket de origem, as seguintes ações ocorrerão por padrão:

- Se você fizer uma solicitação `DELETE` sem especificar um ID de versão de objeto, o S3 no Outposts adicionará um marcador de exclusão. O S3 no Outposts lida com o marcador de exclusão da seguinte forma:
  - O S3 on Outposts não replica o marcador de exclusão por padrão.

  - Porém, você pode adicionar replicação de marcador de exclusão a regras não baseadas em etiquetas. Para obter mais informações sobre como habilitar a replicação do marcador de exclusão na configuração de replicação, consulte Usar o console do S3.
- Se você especificar um ID de versão do objeto para excluir na solicitação `DELETE`, o S3 no Outposts excluirá permanentemente essa versão do objeto no bucket de origem. No entanto, ele não replica a exclusão nos buckets de destino. Em outras palavras: ele não exclui a mesma versão do objeto dos buckets de destino. Esse comportamento protege os dados contra exclusões mal-intencionadas.

O que não é replicado?

Por padrão, o S3 no Outposts não replica o seguinte:

- Objetos no bucket de origem que são réplicas criadas por outra regra de replicação. Por exemplo, se você configurar uma replicação em que o bucket A é a origem e o bucket B é o destino. Agora, suponha que você adicione outra configuração da replicação em que o bucket B é a origem e o bucket C é o destino. Neste caso, os objetos no bucket B que são réplicas de objetos no bucket A não serão replicados para o bucket C.
- Objetos no bucket de origem que já foram replicados para um destino diferente. Por exemplo, se você alterar o bucket de destino em uma configuração de replicação existente, o S3 no Outposts não replicará os objetos novamente.
- Objetos criados com criptografia do lado do servidor com as chaves de criptografia fornecidas pelo cliente (SSE-C).
- Atualizações nos sub-recursos no nível do bucket.

  Por exemplo, se você alterar a configuração do ciclo de vida ou adicionar uma configuração de notificação ao bucket de origem, essas alterações não serão aplicadas ao bucket de destino. Esse recurso torna possível ter configurações diferentes no buckets de origem e de destino.
- Ações realizadas pela configuração do ciclo de vida.

  Por exemplo, se você habilitar uma configuração de ciclo de vida somente no bucket de origem e configurar ações de expiração, o S3 no Outposts criará marcadores de exclusão para objetos expirados no bucket de origem, mas não replicará esses marcadores aos buckets de destino. Se você quiser que a mesma configuração de ciclo de vida seja aplicada aos buckets de origem e de destino, habilite a mesma configuração de ciclo de vida em ambos. Para obter mais informações

sobre a configuração do ciclo de vida, consulte Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts.

O que não é compatível com a replicação do S3 no Outposts?

Os recursos de replicação do S3 a seguir não são compatíveis com o S3 on Outposts:

- Controle de Tempo de Replicação do S3 (S3 RTC). O S3 RTC não é compatível porque o tráfego de objetos na replicação do S3 no Outposts passa pela rede on-premises (o gateway local). Para ter mais informações sobre gateways locais, consulte Trabalhar com o gateway local no Guia do usuário do AWS Outposts.
- Replicação do S3 para operações em lote.

Configuração da replicação

> **Note**
>
> Objetos que já existiam em seu bucket antes de você configurar uma regra de replicação não são replicados automaticamente. Em outras palavras, o Amazon S3 no Outposts não replica os objetos retroativamente. Para replicar objetos que foram criados antes da configuração de replicação, você pode usar a operação da API `CopyObject` para copiá-los no mesmo bucket. Depois que os objetos são copiados, eles aparecem como objetos "novos" no bucket e a configuração de replicação será aplicada a eles. Para ter mais informações sobre como copiar um objeto, consulte Copiar um objeto em um bucket do Amazon S3 no Outposts usando o AWS SDK para Java e CopyObject na Referência da API do Amazon Simple Storage Service.

Para habilitar a replicação do S3 em Outposts, adicione uma regra de replicação ao seu bucket de origem do Outposts. A regra de replicação diz ao S3 no Outposts para replicar objetos, conforme especificado. Na regra de replicação, você deve fornecer o seguinte:

- O ponto de acesso do bucket do Outposts de origem: o nome de recurso da Amazon (ARN) do ponto de acesso ou o alias do ponto de acesso do bucket do qual você deseja que o S3 no Outposts replique os objetos. Para ter mais informações sobre como usar aliases de ponto de acesso, consulte Usar um alias em estilo de bucket para um ponto de acesso de bucket do S3 no Outposts.

- Os objetos que você deseja replicar: você pode replicar todos os objetos do bucket do Outposts de origem ou um subgrupo. Identifique um subgrupo fornecendo, na configuração, um prefixo do nome da chave, uma ou mais tags de objeto ou ambos.

  Por exemplo, se você configurar uma regra de replicação para replicar somente objetos com o prefixo de nome da chave `Tax/`, o S3 no Outposts replicará objetos com chaves como `Tax/doc1` ou `Tax/doc2`. Porém, ele não replica objetos com a chave `Legal/doc3`. Se você especificar um prefixo e uma ou mais tags, o S3 no Outposts replicará somente os objetos com o prefixo das chaves e as tags específicas.
- O bucket do Outposts de destino: o ARN ou o alias do ponto de acesso do bucket para o qual você deseja que o S3 no Outposts replique os objetos.

Você pode configurar a regra de replicação usando a API REST, os AWS SDKs, a AWS Command Line Interface (AWS CLI) ou o console do Amazon S3.

O S3 no Outposts também fornece operações de API para ser compatível com a configuração de regras de replicação. Para obter mais informações, consulte os tópicos a seguir na Referência da API do Amazon Simple Storage Service:

- PutBucketReplication
- GetBucketReplication
- DeleteBucketReplication

Tópicos

- Pré-requisitos para criar regras de replicação
- Criar regras de replicação no Outposts

Pré-requisitos para criar regras de replicação

Tópicos

- Conectar suas sub-redes do Outpost de origem e destino
- Criar uma função do IAM

Conectar suas sub-redes do Outpost de origem e destino

Para que seu tráfego de replicação vá do Outpost de origem para o Outpost de destino pelo gateway local, você deve adicionar uma nova rota para configurar a rede. É necessário conectar os intervalos de rede de Encaminhamento Entre Domínios Sem Classificação (CIDR) de seus pontos de acesso. Para cada par de pontos de acesso, você precisa configurar essa conexão apenas uma vez.

Algumas etapas para configurar a conexão são diferentes, dependendo do tipo de acesso de seus endpoints do Outposts associados aos seus pontos de acesso. O tipo de acesso para endpoints é privado (roteamento direto de nuvem virtual privada [VPC] para AWS Outposts) ou IP de propriedade do cliente (um grupo de endereços IP de propriedade do cliente [grupo de CoIP] em sua rede on-premises).

Etapa 1: Encontrar o intervalo CIDR de seu endpoint do Outposts de origem

Como encontrar o intervalo CIDR de seu endpoint de origem que está associado ao seu ponto de acesso de origem

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Na lista Buckets do Outposts, selecione o bucket de origem desejado para replicação.
4. Selecione a guia Pontos de acesso do Outposts e o ponto de acesso do Outposts do bucket de origem para sua regra de replicação.
5. Selecione endpoint do Outposts.
6. Copie o ID da sub-rede para uso na Etapa 5.
7. O método utilizado para encontrar o intervalo CIDR do endpoint do Outposts de origem depende do tipo de acesso de seu endpoint.

   Na seção Visão geral do endpoint do Outposts, consulte o Tipo de acesso.

   - Se o tipo de acesso for Privado, copie o valor do Encaminhamento Entre Domínios sem Classificação (CIDR) para ser utilizado na Etapa 6.
   - Se o tipo de acesso for IP de propriedade do cliente, faça o seguinte:
     1. Copie o valor do Grupo IPv4 de propriedade do cliente para ser utilizado como ID do grupo de endereços posteriormente.
     2. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.

3. No painel de navegação, selecione Tabelas de rotas do gateway local.
4. Selecione o valor de ID da tabela de rotas do gateway local de seu Outpost de origem.
5. No painel de detalhes, selecione a guia Grupos de CoIP. Cole o valor de seu ID do grupo de CoIP que você copiou anteriormente na caixa de pesquisa.
6. Para o grupo de CoIP correspondente, copie o valor CIDRs correspondente de seu endpoint do Outposts de origem para uso na Etapa 6.

Etapa 2: Encontrar o ID da sub-rede e o intervalo CIDR de seu endpoint do Outposts de destino

Para encontrar o ID da sub-rede e o intervalo CIDR de seu endpoint de destino associado ao seu ponto de acesso de destino, siga as mesmas subetapas indicadas na Etapa 1 e altere seu endpoint do Outposts de origem para o endpoint do Outposts de destino ao realizar essas subetapas. Copie o valor do ID da sub-rede de seu endpoint do Outposts de destino para uso na Etapa 6. Copie o valor CIDR de seu endpoint do Outposts de destino para uso na Etapa 5.

Etapa 3: Encontrar o ID do gateway local do seu Outpost de origem

Como encontrar o ID do gateway local de seu Outpost de origem

1. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.
2. No painel de navegação à esquerda, selecione Gateways locais.
3. Na página Gateways locais, encontre o ID do Outpost de seu Outpost de origem a ser utilizado para replicação.
4. Copie o valor do ID do gateway local de seu Outpost de origem para uso na Etapa 5.

Para ter mais informações sobre o gateway local, consulte Gateway local no Guia do usuário do AWS Outposts.

Etapa 4: Encontrar o ID do gateway local de seu Outpost de destino

Para encontrar o ID do gateway local de seu Outpost de destino, siga as mesmas subetapas indicadas na Etapa 3, exceto para procurar o ID de seu Outpost de destino. Copie o valor do ID do gateway local de seu Outpost de destino para uso na Etapa 6.

Etapa 5: Configurar a conexão da sub-rede do Outpost de origem com a sub-rede do Outpost de destino

Como estabelecer conexão da sub-rede do Outpost de origem com a sub-rede do Outpost de destino

1. Faça login no Console de gerenciamento da AWS e abra o console da VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação à esquerda, escolha Subnets (Sub-redes).
3. Na caixa de pesquisa, insira o ID da sub-rede de seu endpoint do Outposts de origem que você encontrou na Etapa 1. Selecione a sub-rede com o ID de sub-rede correspondente.
4. Para o item de sub-rede correspondente, selecione o valor da tabela de rotas dessa sub-rede.
5. Na página com uma tabela de rotas selecionada, selecione Ações e, depois, Editar rotas.
6. Na página Editar rotas, selecione Editar rota.
7. Em Destino, insira o intervalo CIDR de seu endpoint do Outposts de destino que você encontrou na Etapa 2.
8. Em Destino, selecione Gateway local do Outpost e insira o ID do gateway local de seu Outpost de origem que você encontrou na Etapa 3.
9. Escolha Salvar alterações.
10. O status da rota deve ser ativo.

Etapa 6: Configurar a conexão da sub-rede do Outpost de destino com a sub-rede do Outpost de origem

1. Faça login no Console de gerenciamento da AWS e abra o console da VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação à esquerda, escolha Subnets (Sub-redes).
3. Na caixa de pesquisa, insira o ID da sub-rede de seu endpoint do Outposts de destino que você encontrou na Etapa 2. Selecione a sub-rede com o ID de sub-rede correspondente.
4. Para o item de sub-rede correspondente, selecione o valor da tabela de rotas dessa sub-rede.
5. Na página com uma tabela de rotas selecionada, selecione Ações e, depois, Editar rotas.
6. Na página Editar rotas, selecione Editar rota.
7. Em Destino, insira o intervalo CIDR de seu endpoint do Outposts de origem que você encontrou na Etapa 1.

8. Em Destino, selecione Gateway local do Outpost e insira o ID do gateway local de seu Outpost de destino que você encontrou na Etapa 4.
9. Escolha Salvar alterações.
10. O status da rota deve ser ativo.

Depois de conectar os intervalos de rede CIDR de seus pontos de acesso de origem e destino, você deve criar um perfil do AWS Identity and Access Management (IAM).

Criar uma função do IAM

Por padrão, todos os recursos do S3 no Outposts: buckets, objetos e sub-recursos relacionados, são privados, e somente o proprietário do recurso pode acessá-lo. O S3 no Outposts precisa de permissões de leitura e replicação de objetos a partir do bucket do Outposts de origem. Você concede essas permissões criando um perfil do IAM perfil de serviço e especificando esse perfil na configuração da replicação.

Esta seção explica a política de confiança e a política de permissão mínima necessária. As demonstrações de exemplo fornecem instruções passo a passo para criar uma função do IAM. Para obter mais informações, consulte Criar regras de replicação no Outposts. Para obter mais informações sobre funções do IAM, consulte Funções do IAM no Manual do usuário do IAM.

- O exemplo a seguir mostra uma política de confiança na qual você identifica o S3 no Outposts como a entidade principal do serviço que pode assumir a função.

  JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3-outposts.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

- O exemplo a seguir mostra uma política de acesso em que você concede à função permissões para realizar as tarefas de replicação em seu nome. Quando o S3 no Outposts assumir o perfil, ele terá as permissões que você especificar nessa política. Para utilizar essa política, substitua os *`user input placeholders`* por suas próprias informações. Substitua-os pelos IDs dos Outposts de origem e destino e pelos nomes dos bucket e nomes de pontos de acesso de seus buckets dos Outposts de origem e destino.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3-outposts:GetObjectVersionForReplication",
                "s3-outposts:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3-outposts:us-east-1:123456789012:outpost/SOURCE-
OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET/object/*",
                "arn:aws:s3-outposts:us-east-1:123456789012:outpost/SOURCE-
OUTPOST-ID/accesspoint/SOURCE-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3-outposts:ReplicateObject",
                "s3-outposts:ReplicateDelete"
            ],
            "Resource": [
                "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-
BUCKET/object/*",
                "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/accesspoint/DESTINATION-
OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
            ]
        }
    ]
}
```

A política de acesso concede permissões às seguintes ações:

- `s3-outposts:GetObjectVersionForReplication`: a permissão para essa ação é concedida em todos os objetos para permitir que o S3 no Outposts obtenha uma versão específica associada a cada objeto.

- `s3-outposts:GetObjectVersionTagging`: a permissão para essa ação em objetos no bucket do *`SOURCE-OUTPOSTS-BUCKET`* (o bucket de origem) permite que o S3 no Outposts leia tags de objeto para replicação. Para obter mais informações, consulte Adicionar etiquetas aos buckets do S3 on Outposts. Se o S3 no Outposts não tiver essa permissão, ele replicará os objetos, mas não as tags de objeto.
- `s3-outposts:ReplicateObject` e `s3-outposts:ReplicateDelete`: as permissões para essas ações em todos os objetos no bucket do *`DESTINATION-OUTPOSTS-BUCKET`* (o bucket de destino) permitem que o S3 no Outposts replique objetos ou marcadores de exclusão no bucket do Outposts de destino. Para obter mais informações sobre marcadores de exclusão, consulte Como a exclusão de operações afeta a replicação.

> **Note**
>
> - A permissão para a ação `s3-outposts:ReplicateObject` no bucket do *`DESTINATION-OUTPOSTS-BUCKET`* (o bucket de destino) também permite a replicação de tags de objeto. Portanto, você não precisa conceder permissão explícita para a ação `s3-outposts:ReplicateTags`.
> - Para replicação entre contas, o proprietário do bucket do Outposts de destino deve atualizar sua política de bucket para conceder permissão para a ação `s3-outposts:ReplicateObject` no *`DESTINATION-OUTPOSTS-BUCKET`*. A ação `s3-outposts:ReplicateObject` permite que o S3 no Outposts replique objetos e tags de objetos no bucket do Outposts de destino.

Para obter uma lista das ações do S3 no Outposts, consulte Ações definidas pelo S3 no Outposts.

> **Important**
>
> Mais especificamente, a Conta da AWS proprietária da função do IAM precisa ter permissões para as ações que ela concede à função do IAM.
> Por exemplo, suponha que o bucket do Outposts de origem contenha objetos pertencentes a outra Conta da AWS. O proprietário dos objetos deverá conceder as permissões exigidas

à Conta da AWS proprietária do perfil do IAM por meio da política do bucket e da política de ponto de acesso. Caso contrário, o S3 no Outposts não conseguirá acessar os objetos e ocorrerá uma falha na replicação dos objetos.
As permissões descritas aqui são relativas à configuração mínima da replicação. Se optar por adicionar configurações de replicação opcionais, será necessário conceder permissões adicionais ao S3 no Outposts.

Conceder permissões quando os buckets do Outposts de origem e destino pertencerem a Contas da AWS diferentes

Quando os buckets do Outposts de origem e destino não pertencem às mesmas contas, o proprietário do bucket do Outposts de destino deve atualizar as políticas de bucket e ponto de acesso do bucket de destino. Essas políticas devem conceder ao proprietário do bucket do Outposts de origem e ao perfil de serviço do IAM permissões para realizar ações de replicação, conforme mostrado nos exemplos de políticas a seguir, ou ocorrerá uma falha na replicação. Nestes exemplos de política, *DESTINATION-OUTPOSTS-BUCKET* é o bucket de destino. Para usar esses exemplos de política, substitua os *user input placeholders* por suas próprias informações.

Se você estiver criando o perfil de serviço do IAM manualmente, defina o caminho do perfil como `role/service-role/`, conforme mostrado nos exemplos de políticas a seguir. Para obter mais informações, consulte ARNs do IAM no Guia do usuário do IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "PolicyForDestinationBucket",
    "Statement": [
        {
            "Sid": "Permissions on objects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/source-
account-IAM-role"
            },
            "Action": [
                "s3-outposts:ReplicateDelete",
                "s3-outposts:ReplicateObject"
            ],
```

```
            "Resource": [
                "arn:aws:s3-outposts:us-east-1:444455556666:outpost/DESTINATION-
OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET/object/*"
            ]
        }
    ]
}
```

JSON

```
{
    "Version":"2012-10-17",
    "Id": "PolicyForDestinationAccessPoint",
    "Statement": [
        {
            "Sid": "Permissions on objects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/source-
account-IAM-role"
            },
            "Action": [
                "s3-outposts:ReplicateDelete",
                "s3-outposts:ReplicateObject"
            ],
            "Resource": [
                "arn:aws:s3-outposts:us-east-1:111122223333:outpost/DESTINATION-
OUTPOST-ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
            ]
        }
    ]
}
```

> **Note**
>
> Se os objetos no bucket do Outposts de origem estiverem marcados, observe o seguinte: Se o proprietário do bucket do Outposts de origem conceder ao S3 no Outposts permissão para as ações `s3-outposts:GetObjectVersionTagging` e `s3-outposts:ReplicateTags` para replicação de tags de objeto (pelo perfil do IAM), o

Amazon S3 replicará as tags com os objetos. Para obter informações sobre a função do IAM, consulte Criar uma função do IAM.

Criar regras de replicação no Outposts

A replicação do S3 no Outposts é a replicação assíncrona e automática de objetos em buckets no mesmo AWS Outposts ou em outro. A replicação copia os objetos recém-criados e as atualizações de objeto de um bucket do Outposts de origem para um bucket do Outposts de destino. Para obter mais informações, consulte Replicar objetos para o S3 no Outposts.

> **Note**
>
> Objetos que já existiam no bucket do Outposts de origem antes de você definir regras de replicação não são replicados. Em outras palavras, o S3 no Outposts não replica os objetos retroativamente. Para replicar objetos que foram criados antes da configuração de replicação, você pode usar a operação da API `CopyObject` para copiá-los no mesmo bucket. Depois que os objetos são copiados, eles aparecem como objetos "novos" no bucket e a configuração de replicação será aplicada a eles. Para ter mais informações sobre como copiar um objeto, consulte Copiar um objeto em um bucket do Amazon S3 no Outposts usando o AWS SDK para Java e CopyObject na Referência da API do Amazon Simple Storage Service.

Ao configurar a replicação, você adiciona regras de replicação ao bucket do Outposts de origem. As regras de replicação definem quais objetos do bucket do Outposts de origem devem ser replicados e o bucket do Outposts de destino ou buckets nos quais os objetos replicados são armazenados. Você pode criar uma regra para replicar todos os objetos dentro de um bucket ou um subgrupo de objetos com um prefixo específico de nome de chaves, uma ou mais tags de objetos ou ambos. Um bucket do Outposts de destino pode estar no mesmo Outpost que o bucket do Outposts de origem ou pode estar em outro Outpost.

Para as regras de replicação do S3 no Outposts, você deve fornecer o nome do recurso da Amazon (ARN) do ponto de acesso do bucket do Outposts de origem e o ARN do ponto de acesso do bucket do Outposts de destino em vez dos nomes dos buckets do Outposts de origem e destino.

Se você especificar um ID da versão do objeto a ser excluído, o S3 no Outposts excluirá essa versão do objeto no bucket do Outposts de origem. No entanto, ele não replica a exclusão no bucket do

Outposts de destino. Em outras palavras, ele não exclui a mesma versão do objeto do bucket do Outposts de destino. Esse comportamento protege os dados contra exclusões mal-intencionadas.

Quando você adiciona uma regra de replicação a um bucket do Outposts, ela fica ativada por padrão para que ela comece a funcionar assim que é salva.

Neste exemplo, você configura a replicação para os buckets de origem e destino que estão em Outposts diferentes e pertencem à mesma Conta da AWS. São apresentados exemplos de uso do console do Amazon S3, da AWS Command Line Interface (AWS CLI), do AWS SDK para Java e do AWS SDK para .NET. Para ter informações sobre permissões de replicação do S3 no Outposts entre contas, consulte Conceder permissões quando os buckets do Outposts de origem e destino pertencerem a Contas da AWS diferentes.

Para saber os pré-requisitos para as regras de replicação do S3 no Outposts, consulte Pré-requisitos para criar regras de replicação.

Usar o console do S3

Siga estas etapas para configurar uma regra de replicação quando o bucket do Amazon S3 no Outposts de destino estiver em um Outpost diferente do bucket do Outposts de origem.

Se o bucket do Outposts de destino estiver um uma conta diferente do bucket do Outposts de origem, você deverá adicionar uma política ao bucket do Outposts de destino. Assim, será possível conceder ao proprietário da conta do bucket do Outposts de origem permissão para replicar objetos no bucket do Outposts de destino.

Como criar uma regra de replicação

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets do Outposts, selecione o nome do bucket a ser utilizado como o bucket de origem.
3. Selecione a guia Gerenciamento, role para baixo até a seção Regras de replicação e, depois, selecione Criar regra de replicação.
4. Em Nome da regra de replicação, insira um nome para a regra, ajudando a identificá-la posteriormente. O nome é obrigatório e precisa ser exclusivo dentro do bucket.
5. Em Status, Habilitado é selecionado por padrão. Uma regra ativada começa a funcionar assim que você a salva. Se você quiser ativar a regra posteriormente, selecione Desabilitado.

6. Em Prioridade, o valor da prioridade da regra determina qual regra aplicar se houver regras sobrepostas. Quando objetos são incluídos no escopo de mais de uma regra de replicação, o S3 no Outposts utiliza esses valores de prioridade para evitar conflitos. Por padrão, novas regras são adicionadas à configuração de replicação com a prioridade mais alta. Quanto maior o número, maior a prioridade.

   Para alterar a prioridade da regra, depois de salvá-la, selecione o nome da regra na lista de regras de replicação, selecione Ações e, depois, Editar prioridade.

7. Em Bucket de origem, você tem as seguintes opções para definir a origem da replicação:

   - Para replicar todo o bucket, selecione Aplicar a todos os objetos no bucket.
   - Para aplicar a filtragem de prefixo ou tag à fonte de replicação, selecione Limitar o escopo dessa regra utilizando um ou mais filtros. Você pode combinar um prefixo e tags.
     - Para replicar todos os objetos com o mesmo prefixo, em Prefixo, insira um prefixo na caixa. O uso do filtro Prefixo limita a replicação para todos os objetos que têm nomes que começam com a mesma string (por exemplo, `pictures`).

       Se você inserir um prefixo que seja o nome de uma pasta, use uma / (barra) como o último caractere (por exemplo, `pictures/`).
     - Para replicar todos os objetos que têm uma ou mais tags de objeto, selecione Adicionar tag) e insira o par de chave-valor nas caixas. Para adicionar outra etiqueta, repita o procedimento. Para obter mais informações sobre etiquetas de objeto, consulte Adicionar etiquetas aos buckets do S3 on Outposts.

8. Para acessar seu bucket de origem do S3 no Outposts para replicação, em Nome do ponto de acesso de origem, selecione um ponto de acesso que esteja conectado ao bucket de origem.

9. Em Destino, selecione o ARN do ponto de acesso do bucket do Outposts de destino em que você deseja que o S3 no Outposts replique objetos. O bucket do Outposts de destino pode estar na mesma Conta da AWS que o bucket do Outposts de origem ou em outra.

   Se o bucket de destino estiver um uma conta diferente do bucket do Outposts de origem, você deverá adicionar uma política ao bucket do Outposts de destino. Assim, será possível conceder ao proprietário da conta do bucket do Outposts de origem permissão para replicar objetos no bucket do Outposts de destino. Para obter mais informações, consulte Conceder permissões quando os buckets do Outposts de origem e destino pertencerem a Contas da AWS diferentes.

> **Note**
>
> Se o versionamento não estiver ativado no bucket do Outposts de destino, você receberá um aviso que contém um botão Habilitar versionamento. Escolha esse botão para habilitar o versionamento no bucket.

10. Configure um perfil de serviço do AWS Identity and Access Management (IAM) que o S3 no Outposts possa assumir para replicar objetos em seu nome.

    Para configurar um perfil do IAM, em Perfil do IAM, faça o seguinte:

    - Para que o S3 no Outposts crie um perfil do IAM para sua configuração de replicação, selecione Escolher entre os perfis do IAM existentes e, depois, Criar perfil. Quando você salva a regra, uma nova política é gerada para o perfil do IAM que coincide com os buckets do Outposts de origem e destino que você escolher. Recomendamos que você selecione Criar perfil.
    - Você também pode optar por utilizar um perfil do IAM existente. Se fizer isso, escolha um perfil que conceda ao S3 no Outposts as permissões necessárias para a replicação. Se esse perfil não conceder ao S3 no Outposts permissões suficientes para seguir sua regra de replicação, ocorrerá uma falha na replicação.

      Para selecionar um perfil existente, selecione Escolher entre perfis do IAM existentes e, depois, o perfil no menu suspenso. Você também pode escolher Inserir um ARN de perfil do IAM e, depois, inserir o nome do recurso da Amazon (ARN) do perfil do IAM.

    > **Important**
    >
    > Quando você adiciona uma regra de replicação a um bucket do S3 no Outposts, é preciso ter as permissões `iam:CreateRole` e `iam:PassRole` para poder criar e transmitir o perfil do IAM que concede permissões de replicação do S3 no Outposts. Para ter mais informações, consulte Conceder permissões ao usuário para transmitir um perfil a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

11. Todos os objetos nos buckets do Outposts são criptografados por padrão. Para ter mais informações sobre o S3 no Outposts, consulte Criptografia de dados no S3 on Outposts. Somente objetos que são criptografados com a criptografia no lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) podem ser replicados. A replicação de objetos que são

criptografados com a criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) ou a criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C) não é compatível.

12. Conforme necessário, ative as seguintes opções adicionais ao definir a configuração da regra de replicação:

    - Se você quiser habilitar métricas de replicação do S3 no Outposts na configuração de replicação, selecione Métricas de replicação. Para obter mais informações, consulte Monitorar o andamento com métricas de replicação.
    - Se quiser habilitar a replicação de marcadores de exclusão na configuração de replicação, selecione Delete marker replication (Excluir replicação de marcador). Para obter mais informações, consulte Como a exclusão de operações afeta a replicação.
    - Se você quiser replicar as alterações de metadados feitas nas réplicas de volta aos objetos de origem, selecione Sincronização de modificação de réplica. Para obter mais informações, consulte Status da replicação se a sincronização de modificação de réplica do Amazon S3 no Outposts estiver ativada.

13. Para finalizar, selecione Criar regra.

Depois de salvar sua regra, você pode editar, habilitar, desabilitar ou excluir sua regra. Para fazer isso, acesse a guia Gerenciamento do bucket do Outposts de origem, role para baixo até a seção Regras de replicação, selecione sua regra e Editar regra.

Como usar o AWS CLI

Para usar a AWS CLI para configurar a replicação quando os buckets do Outposts de origem e destino pertencem à mesma Conta da AWS, faça o seguinte:

- Crie os buckets do Outposts de origem e destino.
- Habilite o versionamento nos dois buckets.
- Crie um perfil do IAM que conceda ao S3 permissão para replicar objetos
- Adicione a configuração de replicação ao bucket do Outposts de origem.

Para verificar sua configuração, teste-a.

Como configurar a replicação quando os buckets do Outposts de origem e destino pertencem à mesma Conta da AWS

1. Defina um perfil de credenciais para a AWS CLI. Neste exemplo, usamos o nome de perfil `acctA`. Para ter mais informações sobre a definição de perfis de credencial, consulte Perfis nomeados no Guia do usuário do AWS Command Line Interface.

   > **Important**
   >
   > O perfil que você usar para este exercício deve ter as permissões necessárias. Por exemplo, na configuração da replicação, especifique o perfil de serviço do IAM que o S3 no Outposts pode assumir. Você só poderá fazer isso se o perfil utilizado tiver as permissões `iam:CreateRole` e `iam:PassRole`. Para ter mais informações, consulte Conceder permissões ao usuário para transmitir um perfil a um AWS service (Serviço da AWS) no Guia do usuário do IAM. Se você usar credenciais de administrador para criar um perfil nomeado, este terá a permissão necessária para realizar todas as tarefas.

2. Crie um bucket de origem e habilite o versionamento nele. O comando `create-bucket` a seguir cria um bucket do *`SOURCE-OUTPOSTS-BUCKET`* na região Leste dos EUA (Norte da Virgínia) (`us-east-1`). Para usar esse comando, substitua *`user input placeholders`* por suas informações.

   ```
   aws s3control create-bucket --bucket SOURCE-OUTPOSTS-BUCKET --outpost-id SOURCE-OUTPOST-ID --profile acctA --region us-east-1
   ```

   O comando `put-bucket-versioning` a seguir habilita o versionamento no bucket do *`SOURCE-OUTPOSTS-BUCKET`*. Para usar esse comando, substitua *`user input placeholders`* por suas informações.

   ```
   aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET --versioning-configuration Status=Enabled --profile acctA
   ```

3. Crie um bucket de destino e habilite o versionamento nele. O comando `create-bucket` a seguir cria um bucket do *`DESTINATION-OUTPOSTS-BUCKET`* na região Oeste dos EUA (Oregon) (`us-west-2`). Para usar esse comando, substitua *`user input placeholders`* por suas informações.

> **Note**
>
> Para definir uma configuração da replicação quando os buckets do Outposts de origem e destino estiverem na mesma Conta da AWS, use o mesmo perfil nomeado. Este exemplo usa `acctA`. Para testar a configuração da replicação quando os buckets pertencerem a Contas da AWS distintas, especifique diferentes perfis para cada um.

```
aws s3control create-bucket --bucket DESTINATION-OUTPOSTS-BUCKET --create-bucket-
configuration LocationConstraint=us-west-2 --outpost-id DESTINATION-OUTPOST-ID --
profile acctA --region us-west-2
```

O comando `put-bucket-versioning` a seguir habilita o versionamento no bucket do *DESTINATION-OUTPOSTS-BUCKET*. Para usar esse comando, substitua *user input placeholders* por suas informações.

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-
OUTPOSTS-BUCKET --versioning-configuration Status=Enabled --profile acctA
```

4. Crie um perfil de serviço do IAM. Posteriormente na configuração da replicação, você vai adicionar esse perfil de serviço ao bucket do *SOURCE-OUTPOSTS-BUCKET*. O S3 no Outposts assume esse perfil para replicar objetos em seu nome. A função do IAM é criada em duas etapas:

   a. Criar um perfil do IAM.

      i. Copie a política de confiança a seguir e salve-a em um arquivo chamado `s3-on-outposts-role-trust-policy.json` no diretório atual do computador local. Essa política concede à entidade principal do serviço do S3 no Outposts permissões para assumir o perfil de serviço.

      JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3-outposts.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. Execute o comando da a seguir para criar a função. Substitua *user input placeholders* por suas próprias informações.

```
aws iam create-role --role-name replicationRole --assume-role-policy-
document file://s3-on-outposts-role-trust-policy.json --profile acctA
```

b. Anexe uma política de permissões ao perfil de serviço.

i. Copie a política de permissões a seguir e salve-a em um arquivo com o nome `s3-on-outposts-role-permissions-policy.json` no diretório atual do computador local. Essa política concede permissões para várias ações de bucket e objetos do S3 no Outposts. Para utilizar essa política, substitua os *user input placeholders* por suas próprias informações.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3-outposts:GetObjectVersionForReplication",
                "s3-outposts:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/SOURCE-OUTPOST-ID/bucket/SOURCE-OUTPOSTS-
BUCKET/object/*",
                "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/SOURCE-OUTPOST-ID/accesspoint/SOURCE-
OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3-outposts:ReplicateObject",
                "s3-outposts:ReplicateDelete"
            ],
            "Resource": [
                "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/
bucket/DESTINATION-OUTPOSTS-BUCKET/object/*",
                "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/
accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
            ]
        }
    ]
}
```

ii. Execute o comando a seguir para criar uma política e ligá-la à função. Substitua *user input placeholders* por suas próprias informações.

```
aws iam put-role-policy --role-name replicationRole --policy-
document file://s3-on-outposts-role-permissions-policy.json --policy-
name replicationRolePolicy --profile acctA
```

5. Adicione uma configuração de replicação ao bucket *SOURCE-OUTPOSTS-BUCKET*.

a. Embora a API do S3 no Outposts exija uma configuração de replicação no formato XML, a AWS CLI requer que você especifique a configuração da replicação no formato JSON. Salve o JSON a seguir em um arquivo chamado `replication.json` no diretório local do seu computador. Para usar essa configuração, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": { "Status": "Disabled" },
```

```
      "Filter" : { "Prefix": "Tax"},
      "Destination": {
        "Bucket":
        "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-OUTPOST-
ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT"
      }
    }
  ]
}
```

b. Execute o comando `put-bucket-replication` a seguir para adicionar a configuração de replicação ao seu bucket do Outposts de origem. Para usar esse comando, substitua *`user input placeholders`* por suas informações.

```
aws s3control put-bucket-replication --account-id 123456789012 --
bucket arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-
ID/bucket/SOURCE-OUTPOSTS-BUCKET --replication-configuration file://
replication.json --profile acctA
```

c. Para recuperar a configuração de replicação, use o comando `get-bucket-replication`. Para usar esse comando, substitua *`user input placeholders`* por suas informações.

```
aws s3control get-bucket-replication --account-id 123456789012 --bucket
 arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/
bucket/SOURCE-OUTPOSTS-BUCKET --profile acctA
```

6. Teste a configuração no console do Amazon S3:

a. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

b. No bucket de *`SOURCE-OUTPOSTS-BUCKET`*, crie uma pasta denominada `Tax`.

c. Adicione exemplos de objetos à pasta `Tax` no bucket de *`SOURCE-OUTPOSTS-BUCKET`*.

d. No bucket de *`DESTINATION-OUTPOSTS-BUCKET`*, verifique o seguinte:

- O S3 no Outposts replicou os objetos.

> **Note**
>
> O tempo que o S3 no Outposts leva para replicar um objeto depende do tamanho do objeto. Para obter informações sobre como ver o status da replicação, consulte Obtenção de informações sobre o status da replicação.

- Na guia Propriedades, o Status de replicação está definido como Réplica (identificando-a como um objeto de réplica).

Gerenciar sua replicação

Esta seção descreve opções adicionais de configuração de replicação disponíveis no S3 no Outposts, como determinar o status da replicação e como solucionar problemas de replicação. Para obter informações sobre a configuração de replicação principal, consulte Configuração da replicação.

Tópicos

- Monitorar o andamento com métricas de replicação
- Obtenção de informações sobre o status da replicação
- Solução de problemas de replicação
- Usar o EventBridge para replicação do S3 no Outposts

Monitorar o andamento com métricas de replicação

A replicação do S3 no Outposts fornece métricas detalhadas para as regras de replicação na configuração de replicação. Com métricas de replicação, você pode monitorar em intervalos de cinco minutos o andamento da replicação rastreando bytes pendentes de replicação, latência de replicação e operações pendentes. Para auxiliar na solução de problemas de configuração, você também pode configurar o Amazon EventBridge para receber notificações sobre falhas de replicação.

Quando métricas de replicação são ativadas, a replicação do S3 no Outposts publica as seguintes métricas no Amazon CloudWatch:

- Bytes pendentes de replicação: o número total de bytes de objetos com replicação pendente para determinada regra de replicação.
- Latência de replicação: o número máximo de segundos pelo qual o bucket de destino da replicação está atrás do bucket de origem para determinada regra de replicação.

- Operações pendentes de replicação: o número de operações pendentes de replicação para determinada regra de replicação. As operações incluem objetos, marcadores de exclusão e tags.

> **Note**
>
> As métricas de replicação do S3 no Outposts são cobradas usando a mesma taxa das métricas personalizadas do CloudWatch. Para obter mais informações, consulte Preço do CloudWatch.

Obtenção de informações sobre o status da replicação

O status da replicação pode ajudar você a determinar o estado atual de um objeto que está sendo replicado pelo Amazon S3 no Outposts. O status de replicação de um objeto de origem retornará `PENDING`, `COMPLETED`, ou `FAILED`. O status de replicação de uma réplica retornará `REPLICA`.

Visão geral do status da replicação

Em um cenário de replicação, você tem um bucket de origem em que configura a replicação e um bucket de destino onde o S3 no Outposts replica objetos. Ao solicitar um objeto (usando `GetObject`) ou metadados de objeto (usando `HeadObject`) nesses buckets, o S3 no Outposts retornará o cabeçalho `x-amz-replication-status` na resposta da seguinte maneira:

- Ao solicitar um objeto no bucket de origem, o S3 no Outposts retornará o cabeçalho `x-amz-replication-status` se o objeto em sua solicitação for qualificado para replicação.

  Por exemplo, suponha que, em sua configuração de replicação, você especifique o prefixo de objeto `TaxDocs` para dizer ao S3 no Outposts para replicar somente objetos com o prefixo de nome de chave `TaxDocs`. Todos os objetos dos quais você fizer upload e tiverem esse prefixo de nome de chave, por exemplo, `TaxDocs/document1.pdf`, serão replicados. Para solicitações de objeto com esse prefixo de nome de chave, o S3 no Outposts retorna o cabeçalho `x-amz-replication-status` com um dos seguintes valores para o status de replicação do objeto: `PENDING`, `COMPLETED` ou `FAILED`.

  > **Note**
  >
  > Se a replicação do objeto falhar depois de você fazer upload de um objeto, não será possível tentar novamente a replicação. É preciso fazer upload do objeto novamente.

Os objetos mudam para o estado `FAILED` em caso de problemas como a ausência das permissões da função de replicação ou do bucket. No caso de falhas temporárias, por exemplo, se um bucket ou uma região não estiver disponível, o status da replicação não fará a transição para `FAILED`, mas permanecerá `PENDING`. Depois que o recurso estiver online novamente, o S3 no Outposts retomará a replicação desses objetos.

- Ao solicitar um objeto no bucket de destino, se o objeto de sua solicitação for uma réplica criada pelo S3 no Outposts, o S3 no Outposts retornará o cabeçalho `x-amz-replication-status` com o valor `REPLICA`.

> **Note**
>
> Antes de excluir um objeto de um bucket de origem com a replicação habilitada, verifique o status de replicação dele para garantir que o objeto tenha sido replicado.

Status da replicação se a sincronização de modificação de réplica do Amazon S3 no Outposts estiver ativada

Quando suas regras de replicação ativam a sincronização de modificação de réplica do S3, as réplicas podem informar um status diferente de `REPLICA`. Se alterações de metadados estiverem no processo de replicação, o cabeçalho `x-amz-replication-status` da réplica retornará `PENDING`. Se a sincronização de modificação de réplica não replicar os metadados, o cabeçalho da réplica retornará `FAILED`. Se os metadados forem replicados corretamente, o cabeçalho da réplica retornará o valor `REPLICA`.

Solução de problemas de replicação

Se as réplicas dos objetos não aparecerem no bucket do Amazon S3 no Outposts de destino depois de configurar a replicação, use estas dicas para identificar e corrigir os problemas.

- O tempo que o S3 no Outposts leva para replicar um objeto depende de vários fatores, incluindo a distância entre o Outposts de origem e destino e o tamanho do objeto.

  Você pode conferir o status de replicação do objeto de origem. Se o status de replicação do objeto for `PENDING`, o S3 no Outposts não concluiu a replicação. Se o status de replicação do objeto for `FAILED`, confira a configuração de replicação definida no bucket de origem.
- Na configuração de replicação do bucket de origem, verifique o seguinte:

  - O nome do recurso da Amazon (ARN) do ponto de acesso do bucket de destino está correto.
  - O prefixo do nome de chave está correto. Por exemplo, se você definiu a configuração para replicar objetos com o prefixo `Tax`, apenas objetos com nomes de chaves como `Tax/document1` ou `Tax/document2` serão replicados. Um objeto com o nome de chave `document3` não será replicado.
  - O status é `Enabled`.
- Verifique se o versionamento não foi suspenso em nenhum bucket. Tanto o bucket de origem quanto o de destino devem ter o versionamento ativado.
- Se o bucket de destino pertencer a outra Conta da AWS, verifique se o proprietário do bucket tem uma política de bucket no bucket de destino que permita ao proprietário do bucket de origem replicar objetos. Para ver um exemplo, consulte Conceder permissões quando os buckets do Outposts de origem e destino pertencerem a Contas da AWS diferentes.
- Se a réplica do objeto não aparecer no bucket de destino, os seguintes problemas podem ter impedido a replicação:
  - O S3 no Outposts não replica um objeto em um bucket de origem que seja uma réplica criada por outra configuração de replicação. Por exemplo, se você definir uma configuração de replicação do bucket A para o bucket B e para o bucket C, o S3 no Outposts não replicará réplicas de objetos no bucket B para o bucket C.

    Se você quiser replicar objetos no bucket A para o bucket B e o bucket C, defina vários destinos de bucket em diferentes regras de replicação para sua configuração de replicação do bucket de origem. Por exemplo, crie duas regras de replicação no bucket A de origem, com uma regra para replicar no bucket B de destino e a outra regra para replicar no bucket C.
  - O proprietário do bucket de origem pode conceder a outras Contas da AWS permissão para carregar objetos. Por padrão, o proprietário do bucket de origem não tem nenhuma permissão para os objetos criados por outras contas. A configuração de replicação vai replicar somente os objetos para os quais o proprietário do bucket de origem tem permissões de acesso. Para evitar problemas de replicação, o proprietário do bucket de origem pode conceder a outras Contas da AWS permissões para criar objetos condicionalmente, exigindo permissões explícitas de acesso nesses objetos.
- Vamos supor que, na configuração da replicação, você adicione uma regra para replicar um subconjunto de objetos com uma tag específica. Nesse caso, você deve atribuir a chave da tag específica e o valor no momento de criar o objeto para o S3 no Outposts replicar o objeto. Se você primeiro criar um objeto e depois adicionar a tag ao objeto existente, o S3 no Outposts não replicará o objeto.

- A replicação falhará se a política de bucket negar o acesso à função de replicação para qualquer uma das seguintes ações:

  Bucket de origem:

  ```
  "s3-outposts:GetObjectVersionForReplication",
  "s3-outposts:GetObjectVersionTagging"
  ```

  Buckets de destino:

  ```
  "s3-outposts:ReplicateObject",
  "s3-outposts:ReplicateDelete",
  "s3-outposts:ReplicateTags"
  ```

- O Amazon EventBridge pode notificar você quando os objetos não forem replicados em seus Outposts de destino. Para obter mais informações, consulte Usar o EventBridge para replicação do S3 no Outposts.

Usar o EventBridge para replicação do S3 no Outposts

O Amazon S3 no Outposts é integrado ao Amazon EventBridge e usa o namespace `s3-outposts`. O EventBridge é um serviço de barramento de eventos com tecnologia sem servidor que você pode usar para conectar suas aplicações a dados de diversas origens. Para obter mais informações, consulte O que é Amazon EventBridge? no Manual do Usuário do Amazon EventBridge.

Para auxiliar na solução de problemas de configuração da replicação, você pode configurar o Amazon EventBridge para receber notificações sobre eventos de falha de replicação. O EventBridge pode notificar você em instâncias quando os objetos não forem replicados em seu Outposts de destino. Para ter mais informações sobre o estado atual de um objeto que está sendo replicado, consulte Visão geral do status da replicação.

Sempre que determinados eventos acontecem no bucket do Outposts, o S3 no Outposts pode enviar eventos ao EventBridge. Ao contrário de outros destinos, não é necessário selecionar quais tipos de evento você deseja entregar. Você também pode usar regras do EventBridge para encaminhar eventos para outros destinos. Depois que o EventBridge é ativado, o S3 no Outposts envia todos os eventos a seguir ao EventBridge.

Tipo de evento	Descrição	Namespace
`Operation FailedReplication`	Ocorreu uma falha na replicação de um objeto em uma regra de replicação. Para ter mais informações sobre motivos de falha de replicação do S3 no Outposts, consulte Usar o EventBridge para visualizar os motivos de falha da replicação do S3 no Outposts.	`s3-outposts`

Usar o EventBridge para visualizar os motivos de falha da replicação do S3 no Outposts

A tabela a seguir relaciona os motivos de falha da replicação do S3 no Outposts. Você pode configurar uma regra do EventBridge para publicar e visualizar o motivo da falha por meio do Amazon Simple Queue Service (Amazon SQS), do Amazon Simple Notification Service (Amazon SNS), do AWS Lambda ou do Amazon CloudWatch Logs. Para ter mais informações sobre as permissões que são necessárias para usar esses recursos no EventBridge, consulte Usar políticas com base em recursos para o EventBridge.

Motivos de falha da replicação	Descrição
`AssumeRoleNotPermitted`	O S3 no Outposts não pode assumir o perfil do AWS Identity and Access Management (IAM) especificado na configuração de replicação.
`DstBucketNotFound`	O S3 no Outposts não consegue encontrar o bucket de destino especificado na configuração de replicação.
`DstBucketUnversioned`	O versionamento não está ativado no bucket de destino do Outposts. Para ativar objetos com replicação do S3 no Outposts, você deve ativar o versionamento no bucket de destino.
`DstDelObjNotPermitted`	O S3 no Outposts não consegue replicar exclusões no bucket de destino. A permissão

Motivos de falha da replicação	Descrição
	`s3-outposts:ReplicateDelete` pode estar faltando para o bucket de destino.
`DstMultipartCompleteNotPermitted`	O S3 no Outposts não consegue fazer multipart upload de objetos no bucket de destino. A permissão `s3-outposts:ReplicateObject` pode estar faltando para o bucket de destino.
`DstMultipartInitNotPermitted`	O S3 no Outposts não consegue iniciar um multipart upload de objetos no bucket de destino. A permissão `s3-outposts:ReplicateObject` pode estar faltando para o bucket de destino.
`DstMultipartPartUploadNotPermitted`	O S3 no Outposts não consegue fazer upload de objetos de carregamento fracionado no bucket de destino. A permissão `s3-outposts:ReplicateObject` pode estar faltando para o bucket de destino.
`DstOutOfCapacity`	O S3 no Outposts não consegue se replicar para o Outpost de destino porque o Outposts está sem capacidade de armazenamento do S3.
`DstPutObjNotPermitted`	O S3 no Outposts não consegue replicar objetos no bucket de destino. A permissão `s3-outposts:ReplicateObject` pode estar faltando para o bucket de destino.
`DstPutTaggingNotPermitted`	O S3 no Outposts não consegue replicar tags de objetos no bucket de destino. A permissão `s3-outposts:ReplicateObject` pode estar faltando para o bucket de destino.

Motivos de falha da replicação	Descrição
`DstVersionNotFound`	O S3 no Outposts não consegue encontrar a versão necessária do objeto no bucket de destino para replicar os metadados dessa versão do objeto.
`SrcBucketReplicationConfigMissing`	O S3 no Outposts não consegue encontrar uma configuração de replicação para o ponto de acesso associado ao bucket do Outposts de origem.
`SrcGetObjNotPermitted`	O S3 no Outposts não consegue acessar o objeto no bucket de origem para replicação. A permissão `s3-outposts:GetObjectVersionForReplication` pode estar faltando para o bucket de origem.
`SrcGetTaggingNotPermitted`	O S3 no Outposts não consegue acessar as informações da tag do objeto do bucket de origem. A permissão `s3-outposts:GetObjectVersionTagging` pode estar faltando para o bucket de origem.
`SrcHeadObjectNotPermitted`	O S3 no Outposts não consegue recuperar metadados de objetos do bucket de origem. A permissão `s3-outposts:GetObjectVersionForReplication` pode estar faltando para o bucket de origem.
`SrcObjectNotEligible`	O objeto não é elegível para replicação. O objeto ou suas tags de objeto não correspondem à configuração de replicação.

Para ter mais informações sobre como solucionar erros de replicação, consulte os seguintes tópicos:

- Criar uma função do IAM

- Solução de problemas de replicação

Monitorar o EventBridge com o CloudWatch

Para monitoramento, o Amazon EventBridge é integrado ao Amazon CloudWatch. O EventBridge envia automaticamente métricas ao CloudWatch a cada minuto. Essas métricas incluem o número de eventos que foram correspondidos por uma regra e o número de vezes que um destino é invocado por uma regra. Quando uma regra é executada no EventBridge, todos os destinos associados à regra são invocados. Você pode monitorar o comportamento do EventBridge por meio do CloudWatch das maneiras a seguir.

- Você pode monitorar as métricas disponíveis do EventBridge para suas regras do EventBridge no painel do CloudWatch. Depois, você pode usar os recursos do CloudWatch, como os alarmes do CloudWatch, para definir alarmes em determinadas métricas. Se essas métricas atingirem os valores de limite personalizados que você especificou nos alarmes, você receberá notificações e poderá agir adequadamente.
- Você pode definir o Amazon CloudWatch Logs como destino de sua regra do EventBridge. Depois, o EventBridge cria fluxos de log e o CloudWatch Logs armazena o texto dos eventos como entradas de log. Para ter mais informações, consulte EventBridge and CloudWatch Logs.

Para ter mais informações sobre como depurar eventos de entrega e arquivamento de eventos do EventBridge, consulte os seguintes tópicos:

- Política de repetição de eventos e uso de filas de mensagens não entregues
- Arquivar eventos do EventBridge

Compartilhar o S3 on Outposts usando o AWS RAM

O Amazon S3 on Outposts é compatível com o compartilhamento da capacidade do S3 entre várias contas de uma organização usando o AWS Resource Access Manager (AWS RAM). Com o compartilhamento do S3 on Outposts, você pode permitir que outras pessoas criem e gerenciem buckets, endpoints e pontos de acesso no Outpost.

Este tópico demonstra como usar o AWS RAM para compartilhar o S3 on Outposts e recursos relacionados com outra Conta da AWS da organização da AWS.

Pré-requisitos

- A conta proprietária do Outpost tem uma organização configurada no AWS Organizations. Para obter mais informações, consulte Criar uma organização no Guia do usuário do AWS Organizations.
- A organização inclui a Conta da AWS com a qual você deseja compartilhar a capacidade do S3 on Outposts. Para obter mais informações, consulte Enviar convites para Contas da AWS no Guia do usuário do AWS Organizations.
- Selecione uma das opções a seguir que você deseja compartilhar. O segundo recurso [Subnets (Sub-redes) ou Outposts] deve ser selecionado para que os endpoints também sejam acessíveis. Os endpoints são um requisito de rede para acessar dados armazenados no S3 on Outposts.

Opção 1	Opção 2
S3 on Outposts Permite que o usuário crie buckets no Outposts e pontos de acesso, e adicione objetos a esses buckets.	S3 on Outposts Permite que o usuário crie buckets no Outposts e pontos de acesso, e adicione objetos a esses buckets.
Sub-redes Permite que o usuário use a nuvem privada virtual (VPC) e os endpoints associados à sub-rede.	Outposts Permite que o usuário veja os gráficos de capacidade do S3 e a página inicial do console do AWS Outposts. Também permite que os usuários criem sub-redes em Outposts compartilhados e criem endpoints.

Procedimento

1. Faça login no Console de gerenciamento da AWS usando a Conta da AWS que é proprietária do Outpost, depois abra o console do AWS RAM em https://console.aws.amazon.com/ram/home.
2. Lembre-se de ativar o compartilhamento com o AWS Organizations em AWS RAM. Para obter mais informações, consulte Habilitar compartilhamento de recursos no AWS Organizations no Guia do usuário do AWS RAM.

3. Use a Opção 1 ou a Opção 2 nos pré-requisitos para criar o compartilhamento de um recurso. Se você tiver vários recursos do S3 on Outposts, selecione os nomes de recurso da Amazon (ARNs) dos recursos que você deseja compartilhar. Para ativar endpoints, compartilhe a sub-rede ou o Outpost.

   Para obter mais informações sobre como criar um compartilhamento de recursos, consulte Criar um compartilhamento de recursos no Guia do usuário do AWS RAM.

4. A Conta da AWS com a qual você compartilhou recursos deve agora poder usar o S3 on Outposts. Dependendo da opção que você selecionou em prerequisites (pré-requisitos), forneça as seguintes informações ao usuário da conta:

Opção 1	Opção 2
O ID do Outpost	O ID do Outpost
O ID da VPC	
O ID da sub-rede	
O ID do grupo de segurança	

> **Note**
>
> O usuário pode confirmar que os recursos foram compartilhados com ele usando o console do AWS RAM, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST. O usuário pode visualizar os compartilhamentos de recursos existentes usando o comando get-resource-shares da CLI.

Exemplos de uso

Depois que você compartilha os recursos do S3 on Outposts com outra conta, essa conta pode gerenciar buckets e objetos no Outpost. Se você compartilhou o recurso Subnets (Sub-redes), essa conta poderá usar o endpoint que você criou. Os exemplos a seguir demonstram como um usuário pode usar o AWS CLI para interagir com o Outpost após você compartilhar esses recursos.

Example: criar um bucket

O exemplo a seguir cria um bucket chamado *amzn-s3-demo-bucket1* no Outpost *op-01ac5d28a6a232904*. Antes de usar esse comando, substitua cada *user input placeholder* pelos valores apropriados para seu caso de uso.

```
aws s3control create-bucket --bucket amzn-s3-demo-bucket1 --outpost-
id op-01ac5d28a6a232904
```

Para obter mais informações sobre esse comando, consulte create-bucket na Referência da AWS CLI.

Example: criar um ponto de acesso

O exemplo a seguir cria um ponto de acesso em um Outpost usando os parâmetros de exemplo na tabela a seguir. Antes de usar esse comando, substitua esses valores *user input placeholder* e o código da Região da AWS pelos valores apropriados para o caso de uso.

Parâmetro	Valor
ID da conta	*111122223333*
Nome do ponto de acesso	*example-outpost-access-point*
ID do Outpost	*op-01ac5d28a6a232904*
Nome do bucket do Outpost	*amzn-s3-demo-bucket1*
ID da VPC	*vpc-1a2b3c4d5e6f7g8h9*

> **Note**
>
> O parâmetro Account ID (ID da conta) deve ser o ID da Conta da AWS do proprietário do bucket, que é o usuário compartilhado.

```
aws s3control create-access-point --account-id 111122223333 --name example-outpost-
access-point \
```

```
--bucket arn:aws:s3-outposts:us-east-1:111122223333:outpost/op-01ac5d28a6a232904/
bucket/amzn-s3-demo-bucket1 \
--vpc-configuration VpcId=vpc-1a2b3c4d5e6f7g8h9
```

Para obter mais informações sobre esse comando, consulte create-access-point na Referência da AWS CLI.

Example: carregar um objeto

O exemplo a seguir carrega o arquivo *my_image.jpg* do sistema de arquivos local do usuário em um objeto chamado *images/my_image.jpg* por meio do ponto de acesso *example-outpost-access-point* no Outpost *op-01ac5d28a6a232904*, pertencente à conta da AWS*111122223333*. Antes de usar esse comando, substitua esses valores *user input placeholder* e o código da Região da AWS pelos valores apropriados para o caso de uso.

```
aws s3api put-object --bucket arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/example-outpost-access-
point \
--body my_image.jpg --key images/my_image.jpg
```

Para obter mais informações sobre esse comando, consulte put-object na Referência da AWS CLI.

> **Note**
>
> Se essa operação resultar em um erro Resource not found (Recurso não localizado) ou não responder, pode ser que sua VPC não tenha um endpoint compartilhado.
> Para verificar se há um endpoint compartilhado, use o comando list-shared-endpoints da AWS CLI. Se não houver um endpoint compartilhado, atue com o proprietário do Outpost para criar um. Para obter mais informações, consulte ListSharedEndpoints na Referência da API do Amazon Simple Storage Service.

Example: criar um endpoint

O exemplo a seguir cria um endpoint em um Outpost compartilhado. Antes de usar esse comando, substitua os valores *user input placeholder* para o ID do Outpost, o ID da sub-rede e o ID do grupo de segurança pelos valores apropriados para o caso de uso.

> **Note**
>
> O usuário só poderá executar essa operação se o compartilhamento de recursos incluir o recurso Outposts.

```
aws s3outposts create-endpoint --outposts-id op-01ac5d28a6a232904 --subnet-id XXXXXX --
security-group-id XXXXXXX
```

Para obter mais informações sobre esse comando, consulte create-endpoint na Referência da AWS CLI.

Outros Serviços da AWS que usam o S3 on Outposts

Outros Serviços da AWS que são executados localmente para seu AWS Outposts também podem usar a capacidade do Amazon S3 on Outposts. No Amazon CloudWatch, o namespace `S3Outposts` mostra métricas detalhadas de buckets no S3 on Outposts, mas elas não incluem o uso de outros Serviços da AWS. Para gerenciar a capacidade do S3 on Outposts que é consumida por outros Serviços da AWS, consulte as informações na tabela a seguir.

AWS service (Serviço da AWS)	Descrição	Saiba mais
Amazon S3	Todo uso direto do S3 on Outposts tem uma métrica correspondente de conta e bucket no CloudWatch.	Consulte métricas
Amazon Elastic Block Store (Amazon EBS)	Para o Amazon EBS on Outposts, você pode escolher um AWSOutpost como destino de snapshots e armazená-los localmente no S3 on Outposts.	Saiba mais
Amazon Relationa l Database Service (Amazon RDS)	Você pode usar backups locais do Amazon RDS para armazenar seus backups do RDS localmente no Outpost.	Saiba mais

Monitoramento do S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (OUTPOSTS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte . O que é o Amazon S3 on Outposts?

Para obter mais informações sobre como monitorar sua capacidade de armazenamento do Amazon S3 on Outposts, consulte os tópicos a seguir.

Tópicos

- Como gerenciar a capacidade do S3 no Outposts com as métricas do Amazon CloudWatch
- Como receber notificações de eventos do S3 no Outposts usando o Amazon CloudWatch Events
- Monitoramento do S3 no Outposts com logs do AWS CloudTrail

Como gerenciar a capacidade do S3 no Outposts com as métricas do Amazon CloudWatch

Para ajudar a gerenciar a capacidade fixa do S3 em seu Outpost, recomendamos que você crie alertas do CloudWatch que avisam quando a utilização do armazenamento excede determinado limite. Para obter mais informações sobre as métricas do CloudWatch para o S3 no Outposts, consulte Métricas do CloudWatch. Se não houver espaço suficiente para armazenar um objeto no Outpost, a API retornará uma isenção de capacidade insuficiente (ICE). Para liberar espaço, você pode criar alarmes do CloudWatch que acionam a exclusão explícita de dados ou usar uma política de validade do ciclo de vida para expirar objetos. Para salvar os dados antes da exclusão, você pode usar o AWS DataSync para copiar os dados do Amazon S3 no Outposts para um bucket do S3 em uma Região da AWS. Para obter mais informações sobre como usar o DataSync, consulte Conceitos básicos do AWS DataSync no Guia do usuário do AWS DataSync.

Métricas do CloudWatch

O namespace `S3Outposts` inclui as seguintes métricas para buckets do Amazon S3 em Outposts. É possível monitorar o número total de bytes provisionados do S3 em Outposts, o total de bytes livres disponíveis para objetos e o tamanho total de todos os objetos de determinado bucket. As métricas relacionadas ao bucket ou à conta existem para todo o uso direto do S3. O uso indireto do S3, como o armazenamento de snapshots locais do Amazon Elastic Block Store ou de backups do Amazon Relational Database Service em um Outpost, consome a capacidade do S3, mas não é incluído nas métricas relacionadas ao bucket ou à conta. Para obter mais informações sobre snapshots locais do Amazon EBS, consulte Snapshots locais do Amazon EBS em Outposts. Para ver seu relatório de custos do Amazon EBS, acesse https://console.aws.amazon.com/costmanagement/.

> **Note**
>
> O S3 on Outposts apenas é compatível com as métricas do Amazon S3 a seguir. Como o S3 no Outposts tem um limite de capacidade fixo, recomendamos que você crie alertas do CloudWatch que avisam quando a utilização do armazenamento excede determinado limite.

Métrica	Descrição	Período	Unidades	Tipo
`OutpostTotalBytes`	A capacidade provisionada total em bytes para um Outpost.	5 minutos	Bytes	S3 on Outposts
`OutpostFreeBytes`	A contagem de bytes livres disponíveis em um Outpost para armazenar dados de clientes.	5 minutos	Bytes	S3 on Outposts
`BucketUsedBytes`	O tamanho total de todos os objetos de determinado bucket.	5 minutos	Bytes	S3 no Outposts. Somente uso direto do S3.

Métrica	Descrição	Período	Unidades	Tipo
AccountUsedBytes	O tamanho total de todos os objetos da conta do Outposts especificada.	5 minutos	Bytes	S3 no Outposts. Somente uso direto do S3.
BytesPendingReplication	O número total de bytes de objetos com replicação pendente para determinada regra de replicação. Para obter mais informações sobre como habilitar métricas de replicação, consulte Criar regras de replicação entre Outposts.	5 minutos	Bytes	Opcional. Para replicação do S3 no Outposts.
OperationsPendingReplication	O número total de operações com replicação pendente para uma determinada regra de replicação. Para obter mais informações sobre como habilitar métricas de replicação, consulte Criar regras de replicação entre Outposts.	5 minutos	Contagem	Opcional. Para replicação do S3 no Outposts.
ReplicationLatency	O número atual de atraso em segundos pelo qual o bucket de destino da replicação está atrás do bucket de origem de determinada regra de replicação. Para obter mais informações sobre como habilitar métricas de replicação, consulte Criar regras de replicação entre Outposts.	5 minutos	Segundos	Opcional. Para replicação do S3 no Outposts.

Como receber notificações de eventos do S3 no Outposts usando o Amazon CloudWatch Events

Você pode usar o CloudWatch Events para criar qualquer evento de API do Amazon S3 no Outposts. Ao criar uma regra, você pode optar por receber notificações por meio de todos os destinos compatíveis do CloudWatch, incluindo o Amazon Simple Queue Service (Amazon SQS), o Amazon Simple Notification Service (Amazon SNS) e o AWS Lambda. Para obter mais informações, consulte a lista de serviços da AWS que podem ser destinos para o CloudWatch Events no Guia do usuário do Amazon CloudWatch Events. Para escolher um serviço de destino para trabalhar com o S3 on Outposts, consulte Criar uma regra do CloudWatch Events que é acionada por uma chamada de API da AWS pelo AWS CloudTrail no Guia do usuário do Amazon CloudWatch Events.

> **Note**
>
> Para operações de objeto do S3 no Outposts, os eventos de chamada da AWS API enviados pelo CloudTrail só corresponderão às suas regras se você tiver trilhas (opcionalmente com seletores de eventos) configuradas para receber esses eventos. Para obter mais informações, consulte Trabalhar com arquivos de log do CloudTrail no Guia do usuário do AWS CloudTrail.

Example

Veja a seguir uma regra de amostra para a operação `DeleteObject`. Para usar essa regra de exemplo, substitua *`amzn-s3-demo-bucket1`* pelo nome do bucket do S3 on Outposts.

```
{
  "source": [
    "aws.s3-outposts"
  ],
  "detail-type": [
    "AWS API call through CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "s3-outposts.amazonaws.com"
    ],
    "eventName": [
      "DeleteObject"
```

```
    ],
    "requestParameters": {
      "bucketName": [
        "amzn-s3-demo-bucket1"
      ]
    }
  }
}
```

Monitoramento do S3 no Outposts com logs do AWS CloudTrail

O Amazon S3 no Outposts é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações tomadas por um usuário, uma função ou um AWS service (Serviço da AWS) no S3 no Outposts. Você pode usar o AWS CloudTrail para obter informações sobre o S3 em solicitações no nível de bucket e de objeto do Outposts para auditar e registrar em log sua atividade de eventos do S3 no Outposts.

Para habilitar eventos de dados do CloudTrail para todos os buckets do Outposts ou para uma lista de buckets do Outposts específicos, você deve criar uma trilha manualmente no CloudTrail. Para obter mais informações sobre as entradas do arquivo de log do CloudTrail, consulte Entradas de arquivo de log do S3 no Outposts.

Consulte uma lista completa de eventos de dados do CloudTrail para o S3 no Outposts em Eventos de dados do Amazon S3 no CloudTrail no Guia do usuário do Amazon S3.

> **Note**
>
> - É uma prática recomendada criar uma política de ciclo de vida para o bucket do Outposts de evento de dados do AWS CloudTrail. Configure a política de ciclo de vida para remover periodicamente arquivos de log após o período necessário para auditá-los. Fazer isso reduz a quantidade de dados que o Amazon Athena analisa para cada consulta. Para obter mais informações, consulte Criar e gerenciar uma configuração de ciclo de vida para um bucket do Amazon S3 on Outposts.
> - Para obter exemplos de como consultar logs do CloudTrail, consulte a publicação do Blog sobre big data da AWS Análise da segurança, compatibilidade e atividade operacional usando o AWS CloudTrail e o Amazon Athena.

Habilitar o log do CloudTrail para objetos em um bucket do S3 no Outposts

Você pode usar o console do Amazon S3 para configurar uma trilha do AWS CloudTrail e registrar em log eventos de dados de objetos em um bucket do Amazon S3 no Outposts. O CloudTrail é compatível com o registro em log de operações de API no nível do objeto do S3 no Outposts, como `GetObject`, `DeleteObject` e `PutObject`. Esses eventos são chamados de eventos de dados.

Por padrão, as trilhas do CloudTrail não registram em log eventos de dados. No entanto, é possível configurar trilhas para registrar em log eventos de dados para buckets do S3 no Outposts que você especifica, ou registrar em log eventos para todos os buckets do S3 no Outposts na Conta da AWS.

O CloudTrail não preenche eventos de dados no histórico de eventos do CloudTrail. Além disso, nem todas as operações de API no nível do bucket do S3 no Outposts são preenchidas no histórico de eventos do CloudTrail. Para obter mais informações sobre como consultar os logs do CloudTrail, consulte Usar padrões de filtro do Amazon CloudWatch Logs e o Amazon Athena para consultar logs do CloudTrail no Centro de Conhecimento da AWS.

Para configurar uma trilha para registrar em log eventos de dados para um bucket do S3 no Outposts, você pode usar o console do AWS CloudTrail ou o console do Amazon S3. Se você estiver configurando uma trilha para registrar em log eventos de dados para todos os buckets do S3 no Outposts na sua Conta da AWS, será mais fácil usar o console do CloudTrail. Para obter informações sobre como usar o console do CloudTrail para configurar uma trilha para registrar em log eventos de dados do S3 no Outposts, consulte Eventos de dados no Guia do usuário do AWS CloudTrail.

Important

Há cobranças adicionais para eventos de dados. Para obter mais informações, consulte Definição de preço do AWS CloudTrail.

O procedimento a seguir mostra como usar o console do Amazon S3 para configurar uma trilha do CloudTrail para registrar em log eventos de dados para um bucket do S3 no Outposts.

Note

A proprietária do bucket é a Conta da AWS que o criou e só ela pode configurar eventos de dados do S3 no Outposts a serem enviados ao AWS CloudTrail.

Para habilitar registro de eventos de dados do CloudTrail para um bucket do S3 no Outposts

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Outposts buckets (Buckets do Outposts).
3. Escolha o nome do bucket do Outposts cujos eventos de dados você deseja registrar usando o CloudTrail.
4. Escolha Properties.
5. Na seção Eventos de dados do AWS CloudTrail, escolha Configurar no CloudTrail.

   O console do AWS CloudTrail será aberto.

   Você pode criar uma nova trilha do CloudTrail ou reutilizar uma trilha existente e configurar eventos de dados do S3 no Outposts para serem registrados em sua trilha.
6. Na página Painel do console do CloudTrail, escolha Criar trilha.
7. Na página Etapa 1: escolher atributos da trilha, forneça um nome para a trilha, escolha um bucket do S3 para armazenar logs da trilha, especifique qualquer outras configurações desejadas e escolha Próximo.
8. Na página Etapa 2: escolher eventos de log, em Tipo de evento, escolha Eventos de dados.

   Em Tipo de evento de dados, escolha S3 no Outposts. Escolha Próximo.

   > **Note**
   >
   > - Ao criar uma trilha e configurar o registro em log de eventos de dados para o S3 no Outposts, você deve especificar o tipo de evento de dados corretamente.
   >   - Se você usa o console do CloudTrail, escolha o S3 Outposts para Tipo de evento de dados. Para obter informações sobre como criar trilhas no console do CloudTrail, consulte Criação e atualização de uma trilha com o console no Guia do usuário do AWS CloudTrail. Para obter informações sobre como configurar o registro em log de eventos de dados do S3 no Outposts no console do CloudTrail, consulte Registro em log de eventos de dados para objetos do Amazon S3 no Guia do usuário do AWS CloudTrail.
   >   - Se você usar a AWS Command Line Interface (AWS CLI) ou os AWS SDKs, defina o campo `resources.type` como`AWS::S3Outposts::Object`. Para obter mais informações sobre como registrar em log eventos de dados do S3 no Outposts

com a AWS CLI, consulte Registrar em log eventos do S3 no Outposts no Guia do usuário do AWS CloudTrail.

- Se você usar o console do CloudTrail ou o console do Amazon S3 para configurar uma trilha para registro em log de eventos de dados para um bucket do S3 no Outposts, o console do Amazon S3 mostra que o registro está habilitado no nível do objeto para o bucket.

9. Na página Etapa 3: revisar e criar, revise os atributos da trilha e os eventos de log que você configurou. Depois, escolha Criar trilha.

Para desabilitar o registro de eventos de dados do CloudTrail para objetos em um bucket do S3 no Outposts

1. Faça login no Console de gerenciamento da AWS e abra o console do CloudTrail em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação à esquerda, selecione Trilhas.
3. Escolha o nome da trilha que você criou para registrar em log eventos para o bucket do S3 no Outposts.
4. Na página de detalhes da trilha, escolha Parar o registro no canto superior direito.
5. Na caixa de diálogo exibida, selecione Parar o registro.

Entradas de arquivo de log do AWS CloudTrail do Amazon S3 no Outposts

Os eventos de gerenciamento do Amazon S3 no Outposts estão disponíveis por meio do AWS CloudTrail. Além disso, opcionalmente é possível habilitar o registro em log para eventos de dados no AWS CloudTrail.

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do S3 em uma região que você especifica. Os logs do CloudTrail para buckets do Outposts incluem um novo campo `edgeDeviceDetails`, que identifica o Outpost em que o bucket especificado está localizado.

Campos de log adicionais incluem a ação solicitada, a data e a hora da ação e os parâmetros de solicitação. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação PutObject em `s3-outposts`.


```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/yourUserName",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "yourUserName"
      },
      "eventTime": "2020-11-30T15:44:33Z",
      "eventSource": "s3-outposts.amazonaws.com",
      "eventName": "PutObject",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "26.29.66.20",
      "userAgent": "aws-cli/1.18.39 Python/3.4.10 Darwin/18.7.0 botocore/1.15.39",
      "requestParameters": {
        "expires": "Wed, 21 Oct 2020 07:28:00 GMT",
        "Content-Language": "english",
        "x-amz-server-side-encryption-customer-key-MD5": "wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
        "ObjectCannedACL": "BucketOwnerFullControl",
        "x-amz-server-side-encryption": "Aes256",
        "Content-Encoding": "gzip",
        "Content-Length": "10",
        "Cache-Control": "no-cache",
        "Content-Type": "text/html; charset=UTF-8",
        "Content-Disposition": "attachment",
        "Content-MD5": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
        "x-amz-storage-class": "Outposts",
        "x-amz-server-side-encryption-customer-algorithm": "Aes256",
        "bucketName": "amzn-s3-demo-bucket1",
        "Key": "path/upload.sh"
      },
      "responseElements": {
        "x-amz-server-side-encryption-customer-key-MD5": "wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
        "x-amz-server-side-encryption": "Aes256",
        "x-amz-version-id": "001",
        "x-amz-server-side-encryption-customer-algorithm": "Aes256",
```

```
        "ETag": "d41d8cd98f00b204e9800998ecf8427f"
      },
      "additionalEventData": {
        "CipherSuite": "ECDHE-RSA-AES128-SHA",
        "bytesTransferredIn": 10,
        "x-amz-id-2": "29xXQBV2O
+xOHKItvzY1suLv1i6A52E0zOX159fpfsItYd58JhXwKxXAXI4IQkp6",
        "SignatureVersion": "SigV4",
        "bytesTransferredOut": 20,
        "AuthenticationMethod": "AuthHeader"
      },
      "requestID": "8E96D972160306FA",
      "eventID": "ee3b4e0c-ab12-459b-9998-0a5a6f2e4015",
      "readOnly": false,
      "resources": [
        {
          "accountId": "222222222222",
          "type": "AWS::S3Outposts::Object",
          "ARN": "arn:aws:s3-outposts:us-east-1:YYY:outpost/op-01ac5d28a6a232904/
bucket/path/upload.sh"
        },
        {
          "accountId": "222222222222",
          "type": "AWS::S3Outposts::Bucket",
          "ARN": "arn:aws:s3-outposts:us-east-1:YYY:outpost/op-01ac5d28a6a232904/
bucket/"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": false,
      "recipientAccountId": "444455556666",
      "sharedEventID": "02759a4c-c040-4758-b84b-7cbaaf17747a",
      "edgeDeviceDetails": {
        "type": "outposts",
        "deviceId": "op-01ac5d28a6a232904"
      },
      "eventCategory": "Data"
    }
```

Desenvolver com o Amazon S3 on Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 no AWS Outposts, além de armazenar e recuperar facilmente objetos no local para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. O S3 on Outposts fornece uma nova classe de armazenamento, o S3 Outposts (OUTPOSTS), que usa as APIs do Amazon S3 e é projetado para armazenar dados de forma duradoura e redundante em vários dispositivos e servidores em seu AWS Outposts. Você se comunica com o bucket do Outposts usando um ponto de acesso e uma conexão de endpoint em uma nuvem privada virtual (VPC). É possível usar os mesmos recursos e APIs nos buckets do Outposts da mesma maneira que em buckets do Amazon S3, incluindo políticas de acesso, criptografia e marcação. Só é possível usar o S3 on Outposts por meio do Console de gerenciamento da AWS, da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Para obter mais informações, consulte O que é o Amazon S3 on Outposts?

Os tópicos a seguir fornecem informações sobre desenvolvimento com o S3 on Outposts.

Tópicos

- Regiões compatíveis com o S3 no Outposts
- Operações de API do Amazon S3 on Outposts
- Configurar o cliente de controle do S3 para S3 on Outposts usando o SDK para Java
- Fazer solicitações ao S3 no Outposts por IPv6

Regiões compatíveis com o S3 no Outposts

O S3 no Outposts é compatível com as Regiões da AWS a seguir.

- Leste dos EUA (Norte da Virgínia) (us-east-1)
- Leste dos EUA (Ohio) (us-east-2)
- Oeste dos EUA (Norte da Califórnia) (us-west-1)
- Oeste dos EUA (Oregon) (us-west-2)
- África (Cidade do Cabo) (af-south-1)
- Ásia-Pacífico (Jacarta) (ap-southeast-3)
- Ásia-Pacífico (Mumbai) (ap-south-1)
- Ásia-Pacífico (Osaka) (ap-northeast-3)

- Ásia-Pacífico (Seul) (ap-northeast-2)
- Ásia-Pacífico (Singapura) (ap-southeast-1)
- Ásia-Pacífico (Sydney) (ap-southeast-2)
- Ásia Pacific (Tóquio) (ap-northeast-1)
- Canadá (Central) (ca-central-1)
- Europa (Frankfurt) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londres) (eu-west-2)
- UE (Milão) (eu-south-1)
- Europa (Paris) (eu-west-3)
- UE (Estocolmo) (eu-north-1)
- Israel (Tel Aviv) (il-central-1)
- Oriente Médio (Bahrein) (me-south-1)
- América do Sul (São Paulo) (sa-east-1)
- AWS GovCloud (Leste dos EUA) (us-gov-east-1)
- AWS GovCloud (Oeste dos EUA) (us-gov-wast-1)

Operações de API do Amazon S3 on Outposts

Este tópico lista as operações de API do Amazon S3, do Amazon S3 Control e do Amazon S3 on Outposts que você pode usar com o Amazon S3 on Outposts.

Tópicos

- Operações de API do Amazon S3 para gerenciar objetos
- Operações de API do Amazon S3 Control para gerenciar buckets
- Operações de API do S3 on Outposts para gerenciar Outposts

Operações de API do Amazon S3 para gerenciar objetos

O S3 on Outposts foi projetado para usar as mesmas operações de API de objetos que o Amazon S3. É necessário usar pontos de acesso para acessar qualquer objeto em um bucket do Outpost. Ao usar uma operação de API de objeto com o S3 no Outposts, você fornece o nome do recurso da Amazon (ARN) do ponto de acesso do Outposts ou o alias do ponto de acesso. Para obter mais

informações sobre alias de pontos de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso de bucket do S3 no Outposts.

O Amazon S3 on Outposts é compatível com as seguintes operações de API do Amazon S3:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetObject
- GetObjectTagging
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjects
- ListObjectsV2
- ListObjectVersions
- ListParts
- PutObject
- PutObjectTagging
- UploadPart
- UploadPartCopy

Operações de API do Amazon S3 Control para gerenciar buckets

O S3 on Outposts é compatível com as operações de API a seguir do Amazon S3 Control para lidar com buckets.

- CreateAccessPoint
- CreateBucket

- DeleteAccessPoint
- DeleteAccessPointPolicy
- DeleteBucket
- DeleteBucketLifecycleConfiguration
- DeleteBucketPolicy
- DeleteBucketReplication
- DeleteBucketTagging
- GetAccessPoint
- GetAccessPointPolicy
- GetBucket
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- GetBucketReplication
- GetBucketTagging
- GetBucketVersioning
- ListAccessPoints
- ListRegionalBuckets
- PutAccessPointPolicy
- PutBucketLifecycleConfiguration
- PutBucketPolicy
- PutBucketReplication
- PutBucketTagging
- PutBucketVersioning

Operações de API do S3 on Outposts para gerenciar Outposts

O S3 on Outposts é compatível com as operações de API a seguir do Amazon S3 on Outposts para o gerenciamento de endpoints.

- CreateEndpoint
- DeleteEndpoint
- ListEndpoints

- ListOutpostsWithS3
- ListSharedEndpoints

Configurar o cliente de controle do S3 para S3 on Outposts usando o SDK para Java

No exemplo a seguir, o cliente de controle do Amazon S3 é configurado para o Amazon S3 on Outposts com o uso do AWS SDK para Java. Para usar esse exemplo, substitua cada *`user input placeholder`* por suas próprias informações.

```
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;

public AWSS3Control createS3ControlClient() {

    String accessKey = AWSAccessKey;
    String secretKey = SecretAccessKey;
    BasicAWSCredentials awsCreds = new BasicAWSCredentials(accessKey, secretKey);

    return AWSS3ControlClient.builder().enableUseArnRegion()
            .withCredentials(new AWSStaticCredentialsProvider(awsCreds))
            .build();

}
```

Fazer solicitações ao S3 no Outposts por IPv6

O Amazon S3 no Outposts e os endpoints de pilha dupla do S3 no Outposts oferecem suporte a solicitações para buckets do S3 no Outposts com os protocolos IPv6 e IPv4. Com o suporte a IPv6 para o S3 no Outposts, você pode acessar e operar os buckets e os recursos do ambiente de gerenciamento por meio das APIs do S3 no Outposts em redes IPv6.

> **Note**
>
> As ações em objetos do S3 no Outposts (como `PutObject` ou `GetObject`) não são compatíveis em redes IPv6.

Não há nenhum custo adicional para acessar o S3 no Outposts em redes IPv6. Para obter mais informações sobre o S3 no Outposts, consulte Preços de racks do AWS Outposts.

Tópicos

- Conceitos básicos do IPv6
- Usar endpoints de pilha dupla para fazer solicitações em uma rede IPv6
- Como usar endereços do IPv6 em políticas do IAM
- Testar a compatibilidade com endereços IP
- Usar IPv6 com o AWS PrivateLink
- Usar endpoints de pilha dupla do S3 no Outposts

Conceitos básicos do IPv6

Para fazer uma solicitação a um bucket do S3 no Outposts por IPv6, é necessário usar um endpoint de pilha dupla. A próxima seção descreve como fazer solicitações por meio do IPv6 usando endpoints de pilha dupla.

Veja a seguir algumas considerações importantes antes de tentar acessar um bucket do S3 no Outposts por IPv6:

- O cliente e a rede que estão acessando o bucket devem ter permissão para usar o IPv6.
- As solicitações de estilo hospedado virtual e de estilo de caminho são compatíveis para acessarem o IPv6. Para obter mais informações, consulte Usar endpoints de pilha dupla do S3 no Outposts.
- Se você usar a filtragem de endereços IP de origem nas políticas de usuário do AWS Identity and Access Management (IAM) ou de bucket do S3 no Outposts, será necessário atualizar as políticas para incluir intervalos de endereços IPv6.

  > **Note**
  >
  > Esse requisito se aplica somente às operações de bucket do S3 no Outposts e aos recursos do ambiente de gerenciamento em redes IPv6. As ações em objetos do Amazon S3 no Outposts não são compatíveis em redes IPv6.

- Ao usar o IPv6, os arquivos de log de acesso ao servidor fornecem endereços IP em um formato do IPv6. É necessário atualizar as ferramentas, os scripts e o software existentes que você usa para analisar os arquivos de log do S3 no Outposts, para que eles possam analisar os endereços

IP remotos formatados para IPv6. As ferramentas, os scripts e o software atualizados analisarão corretamente os endereços IP remotos formatados para IPv6.

Usar endpoints de pilha dupla para fazer solicitações em uma rede IPv6

Para fazer solicitações com chamadas de API do S3 no Outposts por IPv6, você pode usar endpoints de pilha dupla pela AWS CLI ou pelo AWS SDK. As operações de API de controle do Amazon S3 e as operações de API do S3 no Outposts funcionam da mesma forma, independentemente de você estar acessando o S3 no Outposts por meio de um protocolo IPv6 ou IPv4. No entanto, lembre-se de que as ações em objetos do S3 no Outposts (como `PutObject` ou `GetObject`) não são compatíveis em redes IPv6.

Ao usar a AWS Command Line Interface (AWS CLI) e os AWS SDKs, você pode utilizar um parâmetro ou um sinalizador para mudar para um endpoint de pilha dupla. Você também pode especificar o endpoint de pilha dupla diretamente como uma substituição do endpoint do S3 no Outposts no arquivo de configuração.

Você pode usar um endpoint de pilha dupla para acessar um bucket do S3 no Outposts por IPv6 de qualquer um dos seguintes:

- A AWS CLI, consulte Usar endpoints de pilha dupla da AWS CLI.
- Os AWS SDKs, consulte Usar endpoints de pilha dupla do S3 no Outposts com os AWS SDKs.

Como usar endereços do IPv6 em políticas do IAM

Antes de tentar acessar um bucket do S3 no Outposts usando um protocolo IPv6, garanta que os usuários do IAM ou as políticas de bucket do S3 no Outposts usadas para filtragem de endereços IP estejam atualizadas para incluir intervalos de endereços IPv6. Se as políticas de filtragem de endereços IP não estiverem atualizadas para lidar com endereços IPv6, você poderá perder o acesso a um bucket do S3 no Outposts ao tentar usar o protocolo IPv6.

As políticas do IAM que filtram endereços IP usam operadores de condição de endereço IP. A política de bucket do S3 no Outposts a seguir identifica o intervalo 54.240.143.* de endereços IPv4 permitidos usando operadores de condição de endereço IP. Todos os endereços IP fora desse intervalo terão o acesso ao bucket do S3 no Outposts negado (`DOC-EXAMPLE-BUCKET`). Como todos os endereços do IPv6 estão fora do intervalo permitido, essa política impede que os endereços do IPv6 possam acessar o `DOC-EXAMPLE-BUCKET`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3-outposts:*",
            "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/OUTPOSTS-ID/bucket/DOC-EXAMPLE-BUCKET/*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "54.240.143.0/24"
                }
            }
        }
    ]
}
```

Você pode modificar o elemento `Condition` da política de bucket do S3 no Outposts para permitir intervalos de endereços IPv4 (`54.240.143.0/24`) e IPv6 (`2001:DB8:1234:5678::/64`), conforme mostrado no exemplo a seguir. Você pode usar o mesmo tipo de bloqueio de `Condition` mostrado no exemplo para atualizar as políticas de usuário e de bucket do IAM.

```
"Condition": {
  "IpAddress": {
     "aws:SourceIp": [
       "54.240.143.0/24",
        "2001:DB8:1234:5678::/64"
      ]
   }
 }
```

Antes de usar o IPv6, você deve atualizar todas as políticas de usuário e de bucket do IAM que usam a filtragem de endereços IP para permitir os intervalos de endereços do IPv6. Recomendamos que você atualize as políticas do IAM com os intervalos de endereços do IPv6 de sua organização além dos intervalos de endereços do IPv4 existentes. Para obter um exemplo de uma política de

bucket que permite acesso por meio do IPv6 e do IPv4, consulte Restringir o acesso a endereços IP específicos.

Você pode revisar suas políticas de usuário do IAM usando o console do IAM em https://console.aws.amazon.com/iam/. Para obter mais informações sobre o IAM, consulte o Manual do usuário do IAM. Para obter informações sobre como editar políticas de bucket do S3 no Outposts, consulte Adicionar ou editar uma política para um bucket do Amazon S3 on Outposts.

Testar a compatibilidade com endereços IP

Se você estiver usando uma instância do Linux ou do Unix ou a plataforma macOS X, poderá testar o acesso a um endpoint de pilha dupla por IPv6. Por exemplo, para testar a conexão com endpoints do Amazon S3 no Outposts via IPv6, use o comando `dig`:

```
dig s3-outposts.us-west-2.api.aws AAAA +short
```

Se o endpoint de pilha dupla em uma rede IPv6 estiver configurado corretamente, o comando `dig` retornará os endereços IPv6 conectados. Por exemplo:

```
dig s3-outposts.us-west-2.api.aws AAAA +short

2600:1f14:2588:4800:b3a9:1460:159f:ebce

2600:1f14:2588:4802:6df6:c1fd:ef8a:fc76

2600:1f14:2588:4801:d802:8ccf:4e04:817
```

Usar IPv6 com o AWS PrivateLink

O S3 no Outposts é compatível com o protocolo IPv6 para serviços e endpoints do AWS PrivateLink. Com o suporte ao AWS PrivateLink para o protocolo IPv6, você pode se conectar aos endpoints de serviço em sua VPC por meio de redes IPv6, tanto de conexões on-premises quanto de outras conexões privadas. O suporte a IPv6 para o AWS PrivateLink para S3 no Outposts também permite a integração do AWS PrivateLink com endpoints de pilha dupla. Para conferir etapas sobre como habilitar o IPv6 para o AWS PrivateLink, consulte Expedite your IPv6 adoption with AWS PrivateLink services and endpoints.

> **Note**
>
> Para atualizar o tipo de endereço IP compatível de IPv4 para IPv6, consulte Modify the supported IP address type no Guia do usuário do AWS PrivateLink.

Usar IPv6 com o AWS PrivateLink

Se você estiver usando o AWS PrivateLink com IPv6, deverá criar um endpoint de interface da VPC IPv6 ou de pilha dupla. Para conferir etapas gerais sobre como criar um endpoint da VPC usando o Console de gerenciamento da AWS, consulte Access an AWS service using an interface VPC endpoint no Guia do usuário do AWS PrivateLink.

Console de gerenciamento da AWS

Use o procedimento a seguir para criar um endpoint de interface da VPC que se conecta ao S3 no Outposts.

1. Faça login no Console de gerenciamento da AWS e abra o console da VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Em Categoria do serviço, escolha Serviços do AWS.
5. Em Nome do serviço, escolha o serviço S3 no Outposts (com.amazonaws.us-east-1.s3-outposts).
6. Em VPC, escolha a VPC de onde você acessará o S3 no Outposts.
7. Em Sub-redes, selecione uma sub-rede por zona de disponibilidade da qual você acessará o S3 no Outposts. Não é possível selecionar várias sub-redes em uma mesma zona de disponibilidade. Será criada uma interface de rede do endpoint para cada sub-rede selecionada. Por padrão, os endereços IP dos intervalos de endereços IP da sub-rede são atribuídos às interfaces de rede do endpoint. Para designar um endereço IP para uma interface de rede do endpoint, selecione Designar endereços IP e insira um endereço IPv6 do intervalo de endereços da sub-rede.
8. Em Tipo de endereço IP, escolha Dualstack. Atribua endereços IPv4 e IPv6 às interfaces de rede do endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.

9. Em Grupos de segurança, selecione os grupos de segurança que deseja associar às interfaces de rede do endpoint para o endpoint da VPC. Por padrão, o grupo de segurança padrão é associado à VPC.
10. Em Política, escolha Acesso total para permitir todas as operações de todas as entidades principais em todos os recursos no endpoint da VPC. Como alternativa, escolha Personalizado para anexar uma política de endpoint da VPC que controle as permissões das entidades principais para realizar ações em recursos pelo endpoint da VPC. Essa opção ficará disponível somente se o serviço for compatível com as políticas de endpoint da VPC. Para obter mais informações, consulte Endpoint policies.
11. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
12. Escolha Criar endpoint.

Example: política de bucket do S3 no Outposts

Para permitir que o S3 no Outposts interaja com os endpoints da VPC, você pode atualizar sua política do S3 no Outposts da seguinte forma:

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3-outposts:*",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
```

AWS CLI

> **Note**
>
> Para habilitar a rede IPv6 em um endpoint da VPC, é necessário definir `IPv6` para o filtro `SupportedIpAddressType` para o S3 no Outposts.

O exemplo a seguir usa o comando `create-vpc-endpoint` para criar um endpoint de interface de pilha dupla.

```
aws ec2 create-vpc-endpoint \
--vpc-id vpc-12345678 \
--vpc-endpoint-type Interface \
--service-name com.amazonaws.us-east-1.s3-outposts \
--subnet-id subnet-12345678 \
--security-group-id sg-12345678 \
--ip-address-type dualstack \
--dns-options "DnsRecordIpType=dualstack"
```

Dependendo da configuração do serviço AWS PrivateLink, as conexões de endpoint recém-criadas talvez precisem ser aceitas pelo provedor de serviços do endpoint da VPC antes de serem usadas. Para obter mais informações, consulte Aceitar ou rejeitar solicitações de conexão no Guia do usuário do AWS PrivateLink.

O exemplo a seguir usa o comando `modify-vpc-endpoint` para atualizar o endpoint da VPC somente IPv para um endpoint de pilha dupla. O endpoint de pilha dupla permite acesso às redes IPv4 e IPv6.

```
aws ec2 modify-vpc-endpoint \
--vpc-endpoint-id vpce-12345678 \
--add-subnet-ids subnet-12345678 \
--remove-subnet-ids subnet-12345678 \
--ip-address-type dualstack \
--dns-options "DnsRecordIpType=dualstack"
```

Para obter mais informações sobre como habilitar a rede IPv6 para o AWS PrivateLink, consulte Expedite your IPv6 adoption with AWS PrivateLink services and endpoints.

Usar endpoints de pilha dupla do S3 no Outposts

Os endpoints de pilha dupla do S3 no Outposts oferecem suporte a solicitações para buckets do S3 no Outposts por IPv6 e IPv4. Esta seção descreve como usar os endpoints de pilha dupla do S3 no Outposts.

Tópicos

- Endpoints de pilha dupla do S3 no Outposts
- Usar endpoints de pilha dupla da AWS CLI
- Usar endpoints de pilha dupla do S3 no Outposts com os AWS SDKs

Endpoints de pilha dupla do S3 no Outposts

Quando você faz uma solicitação para um endpoint de pilha dupla, o URL do bucket do S3 no Outposts é resolvido para um endereço IPv6 ou IPv4. Para obter mais informações sobre como acessar um bucket do S3 no Outposts por IPv6, consulte Fazer solicitações ao S3 no Outposts por IPv6.

Para acessar um bucket do S3 no Outposts por meio de um endpoint de pilha dupla, use um nome de endpoint do tipo caminho. O S3 no Outposts oferece suporte apenas a nomes regionais de endpoint de pilha dupla, o que significa que você deve especificar a região como parte do nome.

Para endpoints FIPS de pilha dupla do tipo caminho, use a seguinte convenção de nomenclatura:

```
s3-outposts-fips.region.api.aws
```

Para endpoints não FIPS de pilha dupla, use a seguinte convenção de nomenclatura:

```
s3-outposts.region.api.aws
```

> **Note**
>
> Os nomes de endpoint do tipo hospedado virtual não são compatíveis com o S3 no Outposts.

Usar endpoints de pilha dupla da AWS CLI

Esta seção fornece exemplos de comandos da AWS CLI usados para fazer solicitações a um endpoint de pilha dupla. Para obter instruções de configuração da AWS CLI, consulte Como começar a usar a AWS CLI e o SDK para Java.

Define o valor de configuração `use_dualstack_endpoint` como `true` em um perfil no arquivo do AWS Config para direcionar todas as solicitações do Amazon S3 feitas pelos comandos `s3` e `s3api` da AWS CLI ao endpoint de pilha dupla para a região especificada. Especifique a região no arquivo de configuração ou em um comando usando a opção `--region`.

Ao usar endpoints de pilha dupla com a AWS CLI, somente o tipo de endereçamento `path` é compatível. O tipo de endereçamento, definido no arquivo de configuração, determina se o nome do bucket está no nome do host ou no URL. Consulte mais informações em s3outposts no Guia de Usuário AWS CLI.

Para usar um endpoint de pilha dupla por meio da AWS CLI, use o parâmetro `--endpoint-url` com o endpoint `http://s3.dualstack.region.amazonaws.com` ou `https://s3-outposts-fips.region.api.aws` em qualquer comando `s3control` ou `s3outposts`.

Por exemplo:

```
$  aws s3control list-regional-buckets --endpoint-url https://s3-
outposts.region.api.aws
```

Usar endpoints de pilha dupla do S3 no Outposts com os AWS SDKs

Esta seção fornece exemplos de como acessar um endpoint de pilha dupla usando os AWS SDKs.

AWS SDK for Java 2.xExemplo do endpoint de pilha dupla do

Os exemplos a seguir mostram como usar as classes `S3ControlClient` e `S3OutpostsClient` para habilitar endpoints de pilha dupla ao criar um cliente do S3 no Outposts usando o AWS SDK for Java 2.x. Para obter instruções sobre como criar e testar um exemplo funcional em Java para o Amazon S3 no Outposts, consulte Como começar a usar a AWS CLI e o SDK para Java.

Example: criar uma classe S3ControlClient com endpoints de pilha dupla habilitados

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListRegionalBucketsRequest;
import software.amazon.awssdk.services.s3control.model.ListRegionalBucketsResponse;
import software.amazon.awssdk.services.s3control.model.S3ControlException;


public class DualStackEndpointsExample1 {

    public static void main(String[] args) {
        Region clientRegion = Region.of("us-east-1");
        String accountId = "111122223333";
        String navyId = "9876543210";

        try {
            // Create an S3ControlClient with dual-stack endpoints enabled.
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                                                             .region(clientRegion)
```

```
                                                                .dualstackEnabled(true)
                                                                .build();
            ListRegionalBucketsRequest listRegionalBucketsRequest =
 ListRegionalBucketsRequest.builder()

       .accountId(accountId)

       .outpostId(navyId)

       .build();

            ListRegionalBucketsResponse listBuckets =
 s3ControlClient.listRegionalBuckets(listRegionalBucketsRequest);
            System.out.printf("ListRegionalBuckets Response: %s%n",
 listBuckets.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 on Outposts
 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        }
        catch (S3ControlException e) {
            // Unknown exceptions will be thrown as an instance of this type.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 on Outposts couldn't be contacted for a response, or the
 client
            // couldn't parse the response from Amazon S3 on Outposts.
            e.printStackTrace();
        }
    }
}
```

Example: criar um S3OutpostsClient com endpoints de pilha dupla habilitados

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3outposts.S3OutpostsClient;
import software.amazon.awssdk.services.s3outposts.model.ListEndpointsRequest;
import software.amazon.awssdk.services.s3outposts.model.ListEndpointsResponse;
import software.amazon.awssdk.services.s3outposts.model.S3OutpostsException;
```

```
public class DualStackEndpointsExample2 {

    public static void main(String[] args) {
        Region clientRegion = Region.of("us-east-1");

        try {
            // Create an S3OutpostsClient with dual-stack endpoints enabled.
            S3OutpostsClient s3OutpostsClient = S3OutpostsClient.builder()
                                                                .region(clientRegion)
                                                                .dualstackEnabled(true)
                                                                .build();
            ListEndpointsRequest listEndpointsRequest =
 ListEndpointsRequest.builder().build();

            ListEndpointsResponse listEndpoints =
 s3OutpostsClient.listEndpoints(listEndpointsRequest);
            System.out.printf("ListEndpoints Response: %s%n",
 listEndpoints.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 on Outposts
 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        }
        catch (S3OutpostsException e) {
            // Unknown exceptions will be thrown as an instance of this type.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 on Outposts couldn't be contacted for a response, or the
 client
            // couldn't parse the response from Amazon S3 on Outposts.
            e.printStackTrace();
        }
    }
}
```

Se você estiver usando o AWS SDK for Java 2.x no Windows, talvez precise definir a seguinte propriedade da máquina virtual Java (JVM):

```
java.net.preferIPv6Addresses=true
```