



Guida per l'utente

Amazon S3 su Outposts.



Versione API 2006-03-01

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon S3 su Outposts.: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discreditì Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è S3 su Outposts?	1
Come funziona S3 su Outposts	1
Regioni	2
Bucket	2
Oggetti	3
Chiavi	3
Funzione Controllo delle versioni S3	4
ID versione	4
Classe di storage e crittografia	4
Policy del bucket	4
Punti di accesso S3 su Outposts	5
Caratteristiche di S3 su Outposts	5
Gestione degli accessi	5
Registrazione e monitoraggio dell'archiviazione	6
Forte coerenza	7
Servizi correlati	7
Accesso a S3 su Outposts	7
Console di gestione AWS	8
AWS Command Line Interface	8
AWSSDK	8
Pagamento per S3 su Outposts	8
Passaggi successivi	9
Configurazione di Outpost	10
Ordine di un nuovo Outpost	10
In che modo S3 su Outposts è diverso	11
Specifiche	11
Operazioni API supportate	12
Comandi API AWS CLI di Amazon S3 supportati da S3 su Outposts	12
Funzionalità Amazon S3 non supportate	12
Limitazioni di rete	13
Guida introduttiva a S3 su Outposts	15
Utilizzo della console S3	15
Creazione di un bucket, un punto di accesso e un endpoint	16
Passaggi successivi	18

Utilizzo di AWS CLI e SDK per Java	19
Fase 1: creazione di un bucket	19
Fase 3: creazione di un punto di accesso	20
Fase 3: creazione di un endpoint	21
Fase 4: caricamento di un oggetto in un bucket S3 su Outposts	22
Reti per S3 su Outposts	23
Scelta del tipo di accesso di rete	23
Accesso a bucket e oggetti S3 su Outposts	23
Gestione delle connessioni tramite interfacce di rete elastiche tra account	24
Utilizzo di bucket S3 su Outposts	25
Bucket	25
Access point	25
Endpoint	26
Operazioni API in S3 su Outposts	26
Creazione e gestione di bucket S3 su Outposts	28
Creazione di un bucket	28
Aggiungere tag	32
Utilizzo delle policy di bucket	34
Aggiunta di una policy di bucket	34
Visualizzazione di una policy del bucket	36
Eliminazione di una policy del bucket	38
Esempi di policy di bucket	39
Elenco di bucket	43
Recupero di un bucket	44
Eliminazione del bucket	46
Utilizzo dei punti di accesso	47
Creazione di un access point	48
Utilizzo di un alias in stile bucket per il punto di accesso	50
Visualizzazione della configurazione del punto di accesso	54
Elenco di punti di accesso	55
Eliminazione di un punto di accesso	56
Aggiunta di una policy del punto di accesso	57
Visualizzazione di una policy del punto di accesso	59
Utilizzo di endpoint	61
Creazione di un endpoint	62
Elenco di endpoint	64

Eliminazione di un endpoint	65
Utilizzo di oggetti S3 su Outposts	67
Caricamento di un oggetto	68
Copia di un oggetto	69
Utilizzo dell'SDK AWS per Java	70
Recupero di un oggetto	71
Elenco degli oggetti	74
Eliminazione di oggetti	77
Utilizzo di HeadBucket	81
Esecuzione di un caricamento in più parti	83
Esecuzione di un caricamento in più parti di un oggetto in un bucket S3 su Outposts	84
Copia di un oggetto in un bucket S3 su Outposts tramite un caricamento in più parti	86
Elencare le parti di un oggetto in un bucket S3 su Outposts	88
Recuperare un elenco di caricamenti in più parti in corso in un bucket S3 su Outposts	90
Utilizzo di URL prefirmati	91
Limitazione delle funzionalità degli URL prefirmati	91
Chi può creare un URL prefirmato	93
Quando S3 su Outposts verifica la data e l'ora di scadenza in un URL prefirmato?	94
Condivisione di oggetti	95
Caricamento di un oggetto	100
Amazon S3 su Outposts con Amazon EMR locale	105
Creazione di un bucket Amazon S3 su Outposts	105
Nozioni di base sull'uso di Amazon EMR con Amazon S3 su Outposts	107
Memorizzazione nella cache di autorizzazione e autenticazione	112
Configurazione della cache di autorizzazione e autenticazione	112
Convalida della firma SigV4A	113
Sicurezza	114
Configurazione di IAM	114
Principi per le policy di S3 su Outposts	117
ARN per S3 su Outposts	117
Esempi di policy per S3 su Outposts	119
Autorizzazioni per gli endpoint	119
Ruoli collegati ai servizi per S3 su Outposts	121
Crittografia dei dati	122
AWS PrivateLink per S3 su Outposts	122
Restrizioni e limitazioni	123

Accesso a endpoint dell'interfaccia S3 su Outposts	124
Aggiornamento di una configurazione DNS locale	126
Creazione di un endpoint VPC	126
Creazione di policy degli endpoint VPC e policy di bucket	126
Chiavi di policy per Signature Version 4 (SigV4)	129
Esempi di policy del bucket che utilizzano chiavi di condizione relative a Signature Version 4	131
Policy gestite da AWS	133
AWSS3OnOutpostsServiceRolePolicy	133
Aggiornamenti delle policy	134
Uso di ruoli collegati ai servizi	134
Autorizzazioni del ruolo collegato ai servizi per S3 su Outposts	135
Creazione di un ruolo collegato ai servizi per S3 su Outposts	138
Modifica di un ruolo collegato ai servizi per S3 su Outposts	138
Eliminazione di un ruolo collegato ai servizi per S3 su Outposts	138
Regioni supportate per i ruoli collegati ai servizi di S3 su Outposts	139
Gestione dello storage S3 su Outposts	140
Gestione del controllo delle versioni S3	140
Creazione e gestione di una configurazione del ciclo di vita	143
Utilizzo della console	143
Utilizzo di AWS CLI e SDK per Java	148
Replica degli oggetti per S3 su Outposts	151
Configurazione di replica	152
Requisiti di Replica Amazon S3 su Outposts	153
Elementi replicati	154
Elementi non replicati	155
Cosa non è supportato da Replica Amazon S3 su Outposts?	156
Impostazione della replica	156
Gestione della replica	176
Condivisione di S3 su Outposts	185
Prerequisiti	185
Procedura	186
Esempi di utilizzo	187
Altri servizi	189
Monitoraggio di S3 su Outposts	191
Metriche CloudWatch	191

Metriche CloudWatch	192
Amazon CloudWatch Events	194
Log di CloudTrail	195
Abilitazione della registrazione CloudTrail per gli oggetti S3 su Outposts	196
Voci del file di log di AWS CloudTrail di Amazon S3 su Outposts	199
Sviluppo con S3 su Outposts	202
Regioni supportate	202
API S3 su Outposts	203
Operazioni API Amazon S3 per la gestione degli oggetti	203
Operazioni API Amazon S3 Control per la gestione dei bucket	204
Operazioni API S3 su Outposts per la gestione di Outposts	205
Configurazione del client di controllo S3	206
Esecuzione di richieste su IPv6	206
Nozioni di base su IPv6	207
Esecuzione di richieste mediante gli endpoint dual-stack	208
Utilizzo degli indirizzi IPv6 nelle policy IAM	208
Test di compatibilità degli indirizzi IP	210
Utilizzo di IPv6 con AWS PrivateLink	210
Utilizzo degli endpoint dual-stack	213

Che cos'è Amazon S3 su Outposts?

AWS Outposts è un servizio completamente gestito che offre la stessa infrastruttura AWS, servizi AWS, API e strumenti praticamente a ogni data center, ambiente in co-locazione o struttura On-Premise per un'esperienza ibrida davvero coerente. AWS Outposts è ideale per carichi di lavoro che richiedono l'accesso in bassa latenza ai sistemi On-Premise, l'elaborazione dei dati locali, la residenza dei dati e la migrazione di applicazioni con interdipendenze del sistema locale. Per ulteriori informazioni, consulta [Che cos'è AWS Outposts?](#) nella Guida per l'utente di AWS Outposts.

Con Amazon S3 su Outposts puoi creare bucket S3 in Outposts e archiviare e recuperare facilmente gli oggetti on-premise. S3 su Outposts fornisce una nuova classe di storage, OUTPOSTS, che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server in Outposts. Comunichi con il bucket Outposts utilizzando un punto di accesso e una connessione di endpoint su un cloud privato virtuale (VPC).

Puoi utilizzare le stesse API e funzionalità sui bucket Outposts come per Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST.

- [Come funziona S3 su Outposts](#)
- [Caratteristiche di S3 su Outposts](#)
- [Servizi correlati](#)
- [Accesso a S3 su Outposts](#)
- [Pagamento per S3 su Outposts](#)
- [Passaggi successivi](#)

Come funziona S3 su Outposts

S3 su Outposts è un servizio di storage di oggetti che consente di archiviare dati come oggetti nei bucket in Outpost. Un oggetto è un file di dati e tutti i metadati che lo descrivono. Un bucket è un container per oggetti o file.

Per archiviare i dati in S3 su Outposts, per prima cosa devi creare un bucket. Quando crei il bucket, ne specifichi il nome e l'Outpost che contiene il bucket. Per accedere al bucket S3 su Outposts ed eseguire le operazioni sugli oggetti, è necessario creare e configurare un punto di accesso. È inoltre necessario creare un endpoint per instradare le richieste al punto di accesso.

I punti di accesso semplificano l'accesso ai dati per qualsiasi Servizio AWS o applicazione del cliente che archivia i dati in S3. I punti di accesso sono endpoint di rete denominati che vengono collegati a bucket che puoi usare per eseguire operazioni su oggetti, ad esempio `GetObject` e `PutObject`. Ogni punto di accesso dispone di autorizzazioni e controlli di rete distinti.

Puoi creare e gestire bucket, punti di accesso ed endpoint S3 su Outposts utilizzando la Console di gestione AWS, AWS CLI, SDK AWS o API REST. Per caricare e gestire oggetti nel bucket S3 su Outposts, puoi utilizzare la AWS CLI, SDK AWS o API REST.

Regioni

Durante il provisioning di AWS Outposts, l'utente o AWS crea una connessione di collegamento del servizio che collega il tuo Outpost alla tua Regione AWS o alla regione interna Outposts per operazioni di bucket e telemetria. Un Outpost si basa sulla connettività con la madre Regione AWS. Il rack Outposts non è progettato per operazioni o ambienti disconnessi con connettività limitata o assente. Per ulteriori informazioni, consulta [Connettività dell'Outpost alle Regioni AWS](#) nella Guida per l'utente di AWS Outposts.

Bucket

Un bucket è un container per gli oggetti archiviati in S3 su Outposts. Puoi archiviare un numero qualsiasi di oggetti in un bucket e avere fino a 100 bucket per account per Outpost.

Quando crei un bucket, inserisci un nome e scegli l'Outpost in cui risiede. Dopo avere creato un bucket, non è possibile modificare il nome del bucket o spostare il bucket in un Outpost diverso. I nomi dei bucket devono seguire le [regole di denominazione dei bucket Amazon S3](#). In S3 su Outposts, i nomi dei bucket sono univoci di un outpost e nell' Account AWS. I bucket S3 su Outposts richiedono `outpost-id`, `account-id` e nome per identificarli.

Il seguente esempio mostra il formato Amazon Resource Name (ARN) per i bucket S3 su Outposts. L'ARN è composto dalla regione di residenza del tuo Outpost, dal tuo account Outpost, dall'ID Outpost e dal nome del bucket.

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

Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. Quando specifichi il bucket per le operazioni di oggetto, utilizza l'ARN o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN del punto di accesso per S3 su Outposts, che include `outpost-id`, `account-id` e il nome del punto di accesso:

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

Per ulteriori informazioni sui bucket, consulta [Utilizzo di bucket S3 su Outposts](#).

Oggetti

Gli oggetti sono le entità fondamentali archiviate in S3 su Outposts. sono composti da dati e metadata. I metadata sono invece un set di coppie nome-valore che descrivono l'oggetto. Queste coppie includono alcuni metadati di default, ad esempio la data dell'ultima modifica, e metadati HTTP standard, come `Content-Type`. È anche possibile specificare metadata personalizzati al momento dell'archiviazione dell'oggetto. Un oggetto viene identificato in modo univoco in un bucket tramite una chiave (nome).

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

Chiavi

Una chiave oggetto (o nome chiave) è l'identificatore univoco di un oggetto in un bucket. Per ogni oggetto in un bucket è presente esattamente una chiave. La combinazione di un bucket e una chiave identifica in modo univoco ciascun oggetto.

Nell'esempio seguente viene illustrato il formato ARN per gli oggetti S3 su Outposts, che include il codice Regione AWS per la regione in cui è ospitato l'Outpost, ID Account AWS, ID Outpost, nome del bucket e chiave dell'oggetto:

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

Per ulteriori informazioni sulle chiavi degli oggetti, consulta [Utilizzo di oggetti S3 su Outposts](#).

Funzione Controllo delle versioni S3

Puoi utilizzare il controllo delle versioni S3 nei bucket Outposts per conservare più versioni di un oggetto nello stesso bucket. Puoi utilizzare Controllo delle versioni S3 per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket. Il controllo delle versioni S3 ti consente di eseguire il ripristino a seguito di errori dell'applicazione e operazioni non intenzionali degli utenti.

Per ulteriori informazioni, consulta [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#).

ID versione

Se abiliti il controllo delle versioni S3 in un bucket, S3 su Outposts genera un ID versione univoco per ciascun oggetto aggiunto al bucket. Gli oggetti già esistenti nel bucket al momento dell'attivazione del controllo delle versioni hanno un ID versione null. Se modifichi questi o altri oggetti con altre operazioni, come [PutObject](#), i nuovi oggetti ottengono un ID versione univoco.

Per ulteriori informazioni, consulta [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#).

Classe di storage e crittografia

S3 su Outposts offre una nuova classe di storage, S3 Outposts (OUTPOSTS). La classe di storage S3 Outposts è disponibile solo per gli oggetti archiviati in bucket su AWS Outposts. Se provi a utilizzare altre classi di storage S3 con S3 su Outposts, S3 su Outposts restituisce l'errore `InvalidStorageClass`.

Gli oggetti archiviati nella classe di storage S3 Outposts (OUTPOSTS) vengono crittografati utilizzando la crittografia lato server con chiavi di crittografia gestite di Amazon S3 (SSE-S3). Per ulteriori informazioni, consulta [Crittografia dei dati in S3 su Outposts](#).

Policy del bucket

Una policy di bucket è una policy AWS Identity and Access Management (IAM) basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni indicate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Le policy di bucket sono limitate a dimensioni di 20 KB.

Le policy di bucket utilizzano la sintassi delle policy IAM basata su JSON, che è lo standard di AWS. Puoi utilizzare policy di bucket per aggiungere o negare autorizzazioni per gli oggetti in un bucket. I criteri del bucket consentono di accettare o rifiutare le richieste in base agli elementi della policy. Questi elementi possono includere richiedente, operazioni S3, risorse e aspetti o condizioni della richiesta (ad esempio, l'indirizzo IP utilizzato per inviarla). Ad esempio, puoi creare una policy che conceda autorizzazioni per gli account per caricare oggetti in un bucket S3 su Outposts garantendo al contempo che il proprietario del bucket abbia il pieno controllo degli oggetti caricati.

Nella policy di bucket puoi utilizzare caratteri jolly (*) negli ARN e altri valori per concedere autorizzazioni a un sottoinsieme di oggetti. Ad esempio, puoi controllare l'accesso a gruppi di oggetti che iniziano con un [prefisso](#) comune o terminano con una determinata estensione, come .html.

Punti di accesso S3 su Outposts

I punti di accesso S3 su Outposts sono endpoint di rete denominati con policy di accesso dedicate che descrivono come è possibile accedere ai dati utilizzando tale endpoint. I punti di accesso semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in S3 su Outposts. I punti di accesso vengono collegati ai bucket che puoi usare per eseguire operazioni su oggetti S3, ad esempio GetObject e PutObject.

Quando specifichi il bucket per le operazioni di oggetto, utilizza l'ARN o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Ogni punto di accesso dispone di autorizzazioni e controlli di rete distinti che S3 su Outposts applica per qualsiasi richiesta effettuata tramite il punto di accesso. Ogni punto di accesso applica una policy personalizzata che funziona insieme alla policy di bucket collegata al bucket sottostante.

Per ulteriori informazioni, consulta [Accesso a bucket e oggetti S3 su Outposts](#).

Caratteristiche di S3 su Outposts

Gestione degli accessi

Amazon S3 offre le caratteristiche per la verifica e la gestione dell'accesso ai bucket e agli oggetti. Per impostazione predefinita, i bucket S3 su Outposts e gli oggetti al loro interno sono privati. Puoi accedere solo alle risorse S3 su Outposts che hai creato.

Per concedere autorizzazioni granulari per le risorse che supportano il tuo caso d'uso specifico o per verificare le autorizzazioni delle tue risorse Amazon S3, puoi utilizzare le seguenti caratteristiche.

- [Blocco dell'accesso pubblico di S3](#): blocca l'accesso pubblico a bucket e oggetti. Per i bucket su Outposts, il blocco dell'accesso pubblico è sempre abilitato per impostazione predefinita.
- [AWS Identity and Access Management \(IAM\)](#): IAM è un servizio Web che aiuta a controllare in modo sicuro l'accesso alle risorse AWS, comprese le risorse S3 su Outposts. Con IAM, puoi gestire a livello centrale le autorizzazioni che controllano le risorse AWS a cui possono accedere gli utenti. Utilizza IAM per controllare chi è autenticato (ha effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse.
- [Punti di accesso S3 su Outposts](#): gestisci l'accesso ai dati per set di dati condivisi in S3 su Outposts. I punti di accesso sono denominati endpoint di rete con policy di accesso dedicate. I punti di accesso vengono collegati ai bucket che puoi usare per eseguire operazioni su oggetti, ad esempio GetObject e PutObject.
- [Policy di bucket](#): utilizza il linguaggio delle policy basato su IAM per configurare le autorizzazioni basate sulle risorse per i bucket S3 e gli oggetti in essi contenuti.
- [AWS Resource Access Manager \(AWS RAM\)](#): condividi in modo sicuro la tua capacità di S3 su Outposts tra gli Account AWS, all'interno della tua organizzazione o unità organizzativa (UO) in AWS Organizations.

Registrazione e monitoraggio dell'archiviazione

S3 su Outposts fornisce strumenti di registrazione e monitoraggio che puoi utilizzare per monitorare e controllare come vengono utilizzate le tue risorse S3 su Outposts. Per ulteriori informazioni, [Strumenti di monitoraggio](#).

- [Parametri di Amazon CloudWatch per S3 su Outposts](#): monitora lo stato operativo delle tue risorse e comprendi la disponibilità della capacità.
- [Eventi Amazon CloudWatch Events per S3 su Outposts](#): crea una regola per ogni evento dell'API S3 su Outposts per ricevere notifiche di tutte le destinazioni supportate di CloudWatch Events, tra cui Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) e AWS Lambda.
- [Log AWS CloudTrail per S3 su Outposts](#): registra le operazioni eseguite da un utente, un ruolo o un Servizio AWS in S3 su Outposts. I registri CloudTrail forniscono il tracking dettagliato delle API per le operazioni a livello di bucket S3 e di oggetto.

Forte coerenza

S3 su Outposts fornisce una coerenza di lettura dopo scrittura per le operazioni PUT e DELETE per gli oggetti nel tuo bucket S3 su Outposts in tutte le Regioni AWS. Questo comportamento vale sia per le scritture dei nuovi oggetti che per le richieste PUT che sovrascrivono gli oggetti esistenti e le richieste DELETE. Inoltre, i tag dell'oggetto S3 su Outposts e i metadati dell'oggetto (ad esempio, l'oggetto HEAD) sono fortemente coerenti. Per ulteriori informazioni, consulta il [modello di coerenza dei dati di Amazon S3](#) nella Guida per l'utente di Amazon S3.

Servizi correlati

Una volta caricati i dati in S3 su Outposts, è possibile utilizzarli con altri Servizi AWS. Di seguito vengono riportati i servizi che potresti utilizzare più di frequente:

- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#): fornisce capacità di calcolo scalabile e sicura in Cloud AWS. L'utilizzo Amazon EC2 riduce la necessità di investimenti anticipati in hardware e ti permette di sviluppare e distribuire più rapidamente le applicazioni. Puoi utilizzare Amazon EC2 per avviare il numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione.
- [Amazon Elastic Block Store \(Amazon EBS\) su Outposts](#): utilizza snapshot locali Amazon EBS su Outposts per archiviare snapshot di volumi in un Outpost localmente in S3 su Outposts.
- [Amazon Relational Database Service \(Amazon RDS\) su Outposts](#): utilizza i backup locali Amazon RDS per archiviare i backup Amazon RDS localmente nel tuo Outpost.
- [AWS DataSync](#): automatizza il trasferimento dei dati tra i tuoi Outposts e le Regioni AWS, scegliendo cosa trasferire, quando trasferire e quanta larghezza di banda della rete utilizzare. S3 su Outposts è integrato con AWS DataSync. Per le applicazioni locali che richiedono un'elaborazione locale ad alta velocità effettiva, S3 su Outposts fornisce archiviazione locale di oggetti in modo da ridurre al minimo i trasferimenti di dati e il buffer dalle variazioni di rete, offrendo al contempo la possibilità di trasferire facilmente i dati tra Outposts e le Regioni AWS.

Accesso a S3 su Outposts

Puoi lavorare con S3 su Outposts nei modi descritti di seguito:

Console di gestione AWS

La console è un'interfaccia utente basata sul Web per la gestione delle risorse S3 su Outposts e AWS. Se ti sei registrato a un account Account AWS, puoi accedere alla console di Amazon S3 accedendo alla Console di gestione AWS e scegliendo S3 dalla home page della Console di gestione AWS. Quindi, scegli Outposts buckets (Bucket Outposts) dal riquadro di navigazione a sinistra.

AWS Command Line Interface

Puoi utilizzare gli strumenti a riga di comando AWS per inviare comandi o creare script per la riga di comando del sistema per eseguire attività AWS (incluso S3).

[AWS Command Line Interface \(AWS CLI\)](#) offre comandi per un'ampia gamma di Servizi AWS. La AWS CLI è supportata su Windows, macOS e Linux. Per iniziare, consulta la [Guida per l'utente di AWS Command Line Interface](#). Per ulteriori informazioni sui comandi utilizzabili con S3 su Outposts, consulta [s3api](#), [s3control](#) e [s3outposts](#) nella Documentazione di riferimento per i comandi AWS CLI.

AWSSDK

AWS fornisce gli SDK (kit di sviluppo software) costituiti da librerie e codice di esempio per vari linguaggi di programmazione e piattaforme (Java, Python, Ruby, .NET, iOS, Android, ecc.). Gli SDK AWS rappresentano un sistema molto comodo per creare un accesso programmatico a S3 su Outposts e AWS. Dal momento che S3 on Outposts utilizza gli stessi SDK di Amazon S3, offre un'esperienza coerente utilizzando API, automazione e strumenti di S3.

S3 on Outposts è un servizio REST. Puoi inviare le richieste a S3 su Outposts utilizzando le librerie di SDK AWS che eseguono il wrapping dell'API REST sottostante, semplificando le attività di programmazione. Ad esempio, gli SDK si occupano di attività quali il calcolo delle firme, la firma crittografica delle richieste, la gestione degli errori e la ripetizione automatica delle richieste. Per ulteriori informazioni sugli SDK AWS, inclusi i dettagli su come scaricarli e installarli, consulta [Strumenti per creare in AWS](#).

Pagamento per S3 su Outposts

È possibile acquistare una varietà di configurazioni rack AWS Outposts con una combinazione di tipi di istanza Amazon EC2, volumi SSD (Solid State Drive) Amazon EBS General Purpose (gp2) e S3 su Outposts. I prezzi includono consegna, installazione e manutenzione del servizio dell'infrastruttura, patch e aggiornamenti software.

Per ulteriori informazioni, consulta [Prezzi del rack AWS Outposts](#).

Passaggi successivi

Per ulteriori informazioni sull'utilizzo di S3 su Outposts, consulta i seguenti argomenti:

- [Configurazione di Outpost](#)
- [In che modo Amazon S3 su Outposts è diverso da Amazon S3?](#)
- [Nozioni di base su Amazon S3 su Outposts](#)
- [Reti per S3 su Outposts](#)
- [Utilizzo di bucket S3 su Outposts](#)
- [Utilizzo di oggetti S3 su Outposts](#)
- [Sicurezza in S3 su Outposts](#)
- [Gestione dello storage S3 su Outposts](#)
- [Sviluppo con Amazon S3 su Outposts](#)

Configurazione di Outpost

Per iniziare a utilizzare Amazon S3 su Outposts, hai bisogno di un Outpost con capacità Amazon S3 distribuita presso la tua struttura. Per informazioni sulle opzioni per ordinare una capacità outpost e S3, vedere [AWS Outposts](#). Per verificare se Outposts ha capacità S3, puoi utilizzare la chiamata API [ListOutpostsWithS3](#). Per le specifiche e per vedere in che modo S3 su Outposts è diverso da Amazon S3, consulta [In che modo Amazon S3 su Outposts è diverso da Amazon S3?](#)

Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

- [Ordine di un nuovo Outpost](#)

Ordine di un nuovo Outpost

Se hai bisogno di ordinare un nuovo Outpost con capacità S3, consulta [Prezzi del rack AWS Outposts](#) per comprendere l'opzione di capacità per Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS) e Amazon S3.

Dopo aver selezionato la configurazione, attieniti alla procedura descritta in [Creare un outpost e ordinare la capacità dell'outpost](#) nella Guida per l'utente di AWS Outposts.

In che modo Amazon S3 su Outposts è diverso da Amazon S3?

Amazon S3 su Outposts fornisce l'archiviazione di oggetti nell'ambiente AWS Outposts on-premise. S3 su Outposts ti consente di soddisfare le esigenze di elaborazione locale, residenza dei dati e prestazioni elevate mantenendo i dati vicini alle applicazioni on-premise. Utilizzando le API e le caratteristiche di Amazon S3, S3 su Outposts semplifica l'archiviazione, la protezione, l'assegnazione di tag, la creazione di report e il controllo dell'accesso ai dati su Outposts ed estende l'infrastruttura AWS alla tua struttura on-premise per un'esperienza ibrida coerente.

Per ulteriori informazioni sull'utilizzo di S3 su Outposts, consulta i seguenti argomenti.

Argomenti

- [Specifiche di S3 su Outposts](#)
- [Operazioni API supportate da S3 su Outposts](#)
- [Comandi API AWS CLI di Amazon S3 supportati da S3 su Outposts](#)
- [Funzionalità Amazon S3 non supportate da S3 su Outposts](#)
- [Requisiti di rete di S3 su Outposts](#)

Specifiche di S3 su Outposts

- La dimensione massima dei bucket Outposts è 50 TB.
- Il numero massimo di bucket Outposts per Account AWS è 100.
- I bucket Outposts sono accessibili solo tramite punti di accesso ed endpoint.
- Il numero massimo di access point per ogni bucket Outposts è 10.
- Le policy access point sono limitate a una dimensione di 20 KB.
- Il proprietario dell'Outpost può gestire l'accesso all'interno dell'organizzazione in AWS Organizations tramite AWS Resource Access Manager. Tutti gli account che devono accedere all'Outpost devono essere all'interno della stessa organizzazione dell'account proprietario in AWS Organizations.
- L'account proprietario del bucket S3 su Outposts è sempre il proprietario di tutti gli oggetti nel bucket.
- Solo l'account proprietario del bucket S3 su Outposts può eseguire operazioni sul bucket.

- Le limitazioni relative alle dimensioni degli oggetti sono coerenti con Amazon S3.
- Tutti gli oggetti archiviati in S3 su Outposts vengono archiviati nella classe di storage OUTPOSTS.
- Per impostazione predefinita, tutti gli oggetti archiviati nella classe di archiviazione OUTPOSTS vengono memorizzati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Puoi inoltre scegliere di archiviare esplicitamente gli oggetti utilizzando la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C).
- Se non c'è spazio sufficiente per archiviare un oggetto sul tuo Outpost, l'API restituirà un'eccezione di capacità insufficiente (ICE).

Operazioni API supportate da S3 su Outposts

Per un elenco di operazioni API supportate da S3 su Outposts, consulta [Operazioni API in Amazon S3 su Outposts](#).

Comandi API AWS CLI di Amazon S3 supportati da S3 su Outposts

I seguenti comandi AWS CLI di Amazon S3 sono al momento supportati da Amazon S3 su Outposts. Per ulteriori informazioni, consulta [Comandi disponibili](#) nella documentazione di riferimento dei comandi della AWS CLI.

- [cp](#), [mv](#), e [sync](#) all'interno dello stesso bucket Outposts o tra un ambiente locale e un bucket Outposts.
- [ls](#)
- [presign](#)
- [rm](#)

Funzionalità Amazon S3 non supportate da S3 su Outposts

Le seguenti funzionalità Amazon S3 al momento non sono supportate da Amazon S3 su Outposts. Tutti i tentativi di utilizzarle vengono rifiutati.

- Richieste condizionali
- Liste di controllo accessi di rete (ACL)
- Cross-Origin Resource Sharing (CORS)
- Operazioni in batch S3

- Report di inventario Amazon S3
- Modifica della crittografia predefinita del bucket
- Bucket pubblici
- Eliminazione dell'autenticazione a più fattori (MFA)
- Transizioni del ciclo di vita di Amazon S3 (a parte l'eliminazione degli oggetti e l'arresto dei caricamenti in più parti incompleti)
- Blocco di carattere legale del blocco oggetti S3
- Conservazione Blocco oggetto
- Crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS)
- S3 Replication Time Control (S3 RTC)
- Parametri delle richieste Amazon CloudWatch
- Configurazione dei parametri
- Transfer Acceleration
- Notifiche di eventi di Amazon S3
- Bucket con Pagamento a carico del richiedente
- S3 Select
- AWS LambdaEventi
- Server access logging (Registrazione degli accessi al server)
- Richieste POST HTTP
- SOAP
- Accesso al sito web

Requisiti di rete di S3 su Outposts

- Per instradare le richieste a un punto di accesso S3 su Outposts, è necessario creare e configurare un endpoint S3 su Outposts. I seguenti limiti si applicano agli endpoint per S3 su Outposts:
 - Ogni cloud privato virtuale (VPC) su un Outpost può avere un endpoint associato, per un massimo di 100 endpoint per Outpost.
 - Puoi mappare più punti di accesso sullo stesso endpoint.
 - Gli endpoint possono essere aggiunti ai VPC solo con blocchi CIDR nei sottospazi dei seguenti intervalli CIDR:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- Gli endpoint di un Outpost possono essere creati solo da VPC che presentano blocchi CIDR che non si sovrappongono.
- Un endpoint può essere creato solo dall'interno della propria sottorete Outposts.
- La sottorete che utilizzi per creare un endpoint deve contenere quattro indirizzi IP utilizzabili da Amazon S3 su Outposts.
- Il pool di indirizzi IP di proprietà del cliente (pool ColP), se specificato, deve contenere quattro indirizzi IP utilizzabili da Amazon S3 su Outposts.
- È possibile creare un solo endpoint per Outpost per VPC.

Nozioni di base su Amazon S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST.

Con Amazon S3 su Outposts è possibile utilizzare le API e le funzionalità Amazon S3, ad esempio l'archiviazione degli oggetti, le policy di accesso, la crittografia e l'aggiunta di tag, su AWS Outposts come si fa su Amazon S3. Per informazioni su S3 su Outposts, consulta [Che cos'è Amazon S3 su Outposts?](#).

Argomenti

- [Nozioni di base per l'utilizzo di Console di gestione AWS](#)
- [Nozioni di base tramite l'utilizzo di AWS CLI e SDK per Java](#)

Nozioni di base per l'utilizzo di Console di gestione AWS

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

Per iniziare a utilizzare S3 su Outposts con la console, consulta i seguenti argomenti. Per le nozioni di base su AWS CLI o AWS SDK per Java, consulta [Nozioni di base tramite l'utilizzo di AWS CLI e SDK per Java](#).

Argomenti

- [Creazione di un bucket, un punto di accesso e un endpoint](#)
- [Passaggi successivi](#)

Creazione di un bucket, un punto di accesso e un endpoint

La procedura seguente mostra come creare il primo bucket in S3 su Outposts. La prima volta che crei un bucket utilizzando la console, crei anche un punto di accesso e un endpoint associato al bucket in modo da poter iniziare immediatamente ad archiviare gli oggetti nel bucket.

1. Accedi alla Console di gestione AWS e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona Crea bucket Outposts.
4. In Bucket name (Nome bucket), immettere un nome conforme a DNS (Domain Name System) per il bucket.

Il nome del bucket deve:

- Essere univoco nell'Account AWS, nell'Outpost e nella Regione AWS in cui si trova l'Outpost.
- Contenere da 3 a 63 caratteri.
- Non contiene caratteri maiuscoli.
- Iniziare con una lettera minuscola o un numero.

Una volta creato il bucket, non è possibile modificarne il nome. Per informazioni sulla denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#) nella Guida per l'utente di Amazon S3.

⚠️ Important

Evitare di includere informazioni riservate, ad esempio numeri di account, nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

5. In Outpost, seleziona l'Outpost in cui desideri sia ospitato il bucket.
6. In Bucket Versioning (Controllo delle versioni del bucket), imposta lo stato del controllo delle versioni S3 per il bucket S3 su Outposts su una delle seguenti opzioni:
 - Disable (Disabilita) (impostazione predefinita): il bucket rimane senza versione.
 - Enable (Abilita): il controllo delle versioni S3 è abilitato per gli oggetti nel bucket. A tutti gli oggetti aggiunti al bucket viene assegnato un ID versione univoco.

Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#).

7. (Opzionale) Aggiungi eventuali tag facoltativi che desideri associare al bucket su Outposts. Puoi utilizzare i tag per monitorare i criteri per singoli progetti o gruppi di progetti, o per etichettare i bucket mediante i tag di allocazione dei costi.

Per impostazione predefinita, tutti gli oggetti archiviati nel bucket su Outposts vengono memorizzati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Puoi inoltre scegliere di archiviare esplicitamente gli oggetti utilizzando la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C). Per modificare il tipo di crittografia, è necessario utilizzare l'API REST, AWS Command Line Interface(AWS CLI) oppure gli SDK AWS.

8. Nella sezione Impostazioni punto di accesso Outposts specifica il nome del punto di accesso.

I punti di accesso S3 su Outposts semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in S3 su Outposts. I punti di accesso sono endpoint di rete denominati che vengono collegati a bucket Outposts che puoi usare per eseguire operazioni su oggetti S3. Per ulteriori informazioni, consulta [Access point](#).

I nomi dei punti di accesso devono essere univoci all'interno dell'account per la Regione e l'outpost e devono rispettare le [restrizioni e limitazioni dei punti di accesso](#).

9. Scegli il VPC per questo access point Amazon S3 su Outposts.

Se non hai un VPC scegli Create VPC (Crea VPC). Per ulteriori informazioni, consulta [Creazione di punti di accesso limitati a un cloud privato virtuale \(VPC\)](#) nella Guida per l'utente di Amazon S3.

Un Virtual Private Cloud (VPC) consente di avviare risorse AWS in una rete virtuale definita dall'utente. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'impiego dell'infrastruttura scalabile di AWS.

10. (Facoltativo per un VPC esistente) Scegli una Endpoint subnet (Subnet endpoint) per l'endpoint.

Una sottorete è un intervallo di indirizzi IP nel VPC. Se non disponi della sottorete desiderata, seleziona Crea sottorete. Per ulteriori informazioni, consulta [Reti per S3 su Outposts](#).

11. (Facoltativo per un VPC esistente) Scegli una Endpoint security group (Gruppo di sicurezza endpoint) per l'endpoint.

Un [gruppo di sicurezza](#) agisce da firewall virtuale per controllare il traffico in entrata e in uscita.

12. (Facoltativo per un VPC esistente) Scegli il Endpoint access type (Tipo di accesso all'endpoint):

- Private (Privato): da utilizzare con il VPC.
- Customer owned IP (IP di proprietà del cliente): da utilizzare con un pool di indirizzi IP di proprietà del cliente all'interno della rete On-Premise.

13. (Facoltativo) Specifica la policy del punto di accesso Outpost. La console visualizza automaticamente l'ARN (Amazon Resource Name del punto di accesso che può essere utilizzato nella policy).

14. Seleziona Crea bucket Outposts.

 Note

Per la creazione dell'endpoint per gli outpost e perché il bucket sia pronto all'uso possono essere necessari fino a 5 minuti. Per configurare ulteriori impostazioni di bucket, seleziona Visualizza dettagli.

Passaggi successivi

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

Dopo aver creato un bucket S3 on Outposts, un punto di accesso e un endpoint, puoi utilizzare AWS CLI o SDK per Java per caricare un oggetto nel bucket. Per ulteriori informazioni, consulta [Caricare un oggetto in un bucket S3 su Outposts](#).

Nozioni di base tramite l'utilizzo di AWS CLI e SDK per Java

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

Per iniziare a utilizzare S3 su Outposts devi creare un bucket, un punto di accesso e un endpoint. Quindi puoi caricare gli oggetti nel bucket. Gli esempi seguenti illustrano come iniziare a utilizzare S3 su Outposts utilizzando AWS CLI e l'SDK per Java. Per le nozioni di base sulla console, consulta [Nozioni di base per l'utilizzo di Console di gestione AWS](#).

Argomenti

- [Fase 1: creazione di un bucket](#)
- [Fase 3: creazione di un punto di accesso](#)
- [Fase 3: creazione di un endpoint](#)
- [Fase 4: caricamento di un oggetto in un bucket S3 su Outposts](#)

Fase 1: creazione di un bucket

Gli esempi seguenti illustrano come creare un bucket S3 su Outposts utilizzando AWS CLI e SDK per Java.

AWS CLI

Example

L'esempio seguente crea un bucket S3 su Outposts (`s3-outposts:CreateBucket`) utilizzando la AWS CLI. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

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

SDK for Java

Example

Per esempi di come creare un bucket S3 Outposts con il kit AWS SDK per Java, [consulta `CreateOutpostsBucket.java`](#) in Esempi di codice AWS SDK per Java 2.x.

Fase 3: creazione di un punto di accesso

Per accedere al bucket Amazon S3 su Outposts devi creare e configurare un punto di accesso. Questi esempi illustrano come creare un punto di accesso utilizzando AWS CLI e l'SDK per Java.

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti di Amazon S3, ad esempio `GetObject` e `PutObject`. Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. I punti di accesso supportano solo l'indirizzamento in stile hosting virtuale.

AWS CLI

Example

Nell'esempio della AWS CLI seguente viene creato un punto di accesso per un bucket di Outposts. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
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

Per esempi di come creare un punto di accesso per un bucket S3 Outposts con il kit AWS SDK per Java, consulta [CreateOutpostsAccessPoint.java](#) in Esempi di codice SDK AWS per Java 2.x.

Fase 3: creazione di un endpoint

Per instradare le richieste verso un punto di accesso Amazon S3 su Outposts, è necessario creare e configurare un endpoint S3 su Outposts. Per creare un endpoint, è necessario disporre di una connessione attiva con il collegamento del servizio alla regione di origine degli outpost. Ogni cloud privato virtuale (VPC) del tuo Outpost può avere un endpoint associato. Per ulteriori informazioni sull'endpoint, consulta [Requisiti di rete di S3 su Outposts](#). È necessario creare un endpoint per poter accedere ai bucket Outposts ed eseguire operazioni sugli oggetti. Per ulteriori informazioni, consulta [Endpoint](#).

Questi esempi illustrano come creare un endpoint utilizzando AWS CLI e SDK per Java. Per ulteriori informazioni sulle autorizzazioni richieste per la creazione e la gestione degli endpoint, consulta [Autorizzazioni per endpoint S3 su Outposts](#).

AWS CLI

Example

Nel seguente esempio AWS CLI viene creato un endpoint per un Outpost utilizzando il tipo di accesso alle risorse del VPC. Il VPC deriva dalla sottorete. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

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

Nel seguente esempio AWS CLI viene creato un endpoint per un Outpost utilizzando il tipo di accesso al pool di indirizzi IP di proprietà del cliente (pool ColIP). Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
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

Per esempi su come creare un endpoint per un S3 Outpost con il kit AWS SDK per Java, consulta [CreateOutpostsEndPoint.java](#) in Esempi di codice AWS SDK per Java 2.x.

Fase 4: caricamento di un oggetto in un bucket S3 su Outposts

Per caricare un oggetto, consulta [Caricare un oggetto in un bucket S3 su Outposts](#).

Reti per S3 su Outposts

Puoi utilizzare S3 su Outposts per archiviare e recuperare oggetti On-Premise per le applicazioni che richiedono l'accesso ai dati locali, l'elaborazione dei dati e la residenza dei dati. Questa sezione descrive i requisiti di rete per l'accesso a S3 su Outposts.

Argomenti

- [Scelta del tipo di accesso di rete](#)
- [Accesso a bucket e oggetti S3 su Outposts](#)
- [Interfacce di rete elastiche tra account](#)

Scelta del tipo di accesso di rete

Puoi accedere a S3 su Outposts dall'interno di un VPC o dalla tua rete on-premise. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint. In tal modo il traffico tra il tuo VPC e i bucket S3 on Outposts viene mantenuto all'interno della rete AWS. Quando crei un endpoint, devi specificare il tipo di accesso all'endpoint tra **Private** (per l'instradamento al VPC) e **CustomerOwnedIp** (per il pool di indirizzi IP di proprietà del cliente [pool CoIP]).

- **Private** (per l'instradamento al VPC). Se non indichi il tipo di accesso, S3 su Outposts utilizza **Private** per impostazione predefinita. Con il tipo di accesso **Private**, le istanze nel VPC non richiedono indirizzi IP pubblici per comunicare con le risorse nell'Outpost. Puoi lavorare con S3 su Outposts da un VPC. Questo tipo di endpoint è accessibile dalla rete on-premise attraverso il routing VPC diretto. Per ulteriori informazioni, consulta [Local gateway route tables](#) nella Guida per l'utente di AWS Outposts.
- **CustomerOwnedIp** (per il pool CoIP). Se non usi il valore predefinito tipo di accesso **Private** e scegli **CustomerOwnedIp**, devi specificare un intervallo di indirizzi IP. Puoi utilizzare questo tipo di accesso per lavorare con S3 su Outposts dalla rete On-Premise e in un VPC. Quando accedi a S3 su Outposts all'interno di un VPC, il traffico è limitato alla larghezza di banda del gateway locale.

Accesso a bucket e oggetti S3 su Outposts

Per accedere ai tuoi oggetti e ai bucket di S3 su Outposts, devi disporre di:

- Un punto di accesso per il VPC.

- Un endpoint per lo stesso VPC.
- Una connessione attiva tra il tuo Outpost e la tua Regione AWS. Per ulteriori informazioni su come connettere l'outpost a una regione, consulta [Outpost connectivity to AWS Regions](#) nella Guida per l'utente di AWS Outposts.

Per ulteriori informazioni sull'accesso a bucket e oggetti in S3 su Outposts, consulta [Utilizzo di bucket S3 su Outposts](#) e [Utilizzo di oggetti S3 su Outposts](#).

Interfacce di rete elastiche tra account

Gli endpoint S3 su Outposts sono risorse denominate con ARN (Amazon Resource Name). Quando vengono creati questi endpoint, AWS Outposts imposta quattro interfacce di rete elastiche tra account. Le interfacce di rete elastiche tra account S3 su Outposts sono come altre interfacce di rete con una sola eccezione: S3 su Outposts associa le interfacce di rete elastiche tra account alle istanze Amazon EC2.

Il DNS (Domain Name System) di S3 su Outposts userà il bilanciamento del carico delle tue richieste sull'interfaccia di rete elastica tra account. S3 su Outposts crea l'interfaccia di rete elastica tra account nel tuo account AWS, visibile dal riquadro Interfacce di rete della console Amazon EC2.

Per gli endpoint che utilizzano il tipo di accesso al pool ColP, S3 su Outposts alloca e associa gli indirizzi IP all'interfaccia di rete elastica tra account dal pool ColP configurato.

Utilizzo di bucket S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti On-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di storage, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

Comunichi con i bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Per accedere ai tuoi oggetti e bucket S3 su Outposts, devi disporre di un punto di accesso per il VPC e di un endpoint per lo stesso VPC. Per ulteriori informazioni, consulta [Reti per S3 su Outposts](#).

Bucket

In S3 su Outposts, i nomi dei bucket sono univoci in un Outpost e richiedono il codice Regione AWS per la regione in cui è presente Outpost, l'ID Account AWS, l'ID Outpost e il nome del bucket per identificarli.

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

Per ulteriori informazioni, consulta [ARN delle risorse per S3 su Outposts](#).

Access point

Amazon S3 su Outposts supporta i punti di accesso configurati solo per i virtual private cloud (VPC) come unico mezzo per accedere ai bucket di Outposts.

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti di Amazon S3, ad esempio GetObject e PutObject. Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. I punti di accesso supportano solo l'indirizzamento in stile hosting virtuale.

Il seguente esempio illustra il formato ARN da utilizzare per i punti di accesso di S3 su Outposts. L'ARN del punto di accesso il codice Regione AWS per la regione in cui è presente l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso.

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

Endpoint

Per instradare le richieste a un punto di accesso S3 su Outposts, è necessario creare e configurare un endpoint S3 su Outposts. Con gli endpoint S3 su Outposts, puoi collegare privatamente il tuo VPC al tuo bucket Outpost. Gli endpoint S3 su Outposts sono URI (Uniform Resource Identifier) virtuali del punto di ingresso al bucket S3 su Outposts. Sono componenti VPC con scalabilità orizzontale, ridondanza e disponibilità elevata.

Ogni cloud privato virtuale (VPC) del tuo Outpost può avere un endpoint associato, per un massimo di 100 endpoint per Outpost. È necessario creare questi endpoint per poter accedere ai bucket Outpost ed eseguire operazioni sugli oggetti. La creazione di questi endpoint consente inoltre che il modello API e i comportamenti siano gli stessi consentendo alle stesse operazioni di funzionare in S3 e S3 su Outposts.

Operazioni API in S3 su Outposts

S3 su Outposts ospita un endpoint separato diverso dall'endpoint Amazon S3 per gestire le operazioni API del bucket Outpost. Questo endpoint è `s3-outposts.region.amazonaws.com`.

Per utilizzare le operazioni API Amazon S3, è necessario firmare il bucket e gli oggetti utilizzando il formato ARN corretto. Gli ARN per le operazioni API vanno inoltrati in modo che Amazon S3 possa determinare se la richiesta è per Amazon S3 (`s3-control.region.amazonaws.com`) o per S3 su Outposts (`s3-outposts.region.amazonaws.com`). In base al formato dell'ARN, S3 può quindi firmare e instradare la richiesta in modo appropriato.

Ogni volta che la richiesta viene inviata al pannello di controllo Amazon S3, l'SDK estrae i componenti dall'ARN e include l'intestazione aggiuntiva `x-amz-outpost-id` con il valore `outpost-id` estratto dall'ARN. Il nome del servizio dall'ARN verrà utilizzato per firmare la richiesta prima che venga instradata all'endpoint S3 su Outposts. Questo comportamento si applica a tutte le operazioni API gestite dal client `s3control`.

Nella tabella seguente sono riportate le operazioni API estese per Amazon S3 su Outposts e le loro modifiche rispetto ad Amazon S3.

API	S3 sul valore del parametro Outposts
CreateBucket	Nome bucket come ARN, ID Outpost
ListRegionalBuckets	ID Outpost
DeleteBucket	Nome del bucket come ARN
DeleteBucketLifecycleConfiguration	Nome del bucket come ARN
GetBucketLifecycleConfiguration	Nome del bucket come ARN
PutBucketLifecycleConfiguration	Nome del bucket come ARN
GetBucketPolicy	Nome del bucket come ARN
PutBucketPolicy	Nome del bucket come ARN
DeleteBucketPolicy	Nome del bucket come ARN
GetBucketTagging	Nome del bucket come ARN
PutBucketTagging	Nome del bucket come ARN
DeleteBucketTagging	Nome del bucket come ARN
CreateAccessPoint	Nome del punto di accesso come ARN
DeleteAccessPoint	Nome del punto di accesso come ARN

API	S3 sul valore del parametro Outposts
GetAccessPoint	Nome del punto di accesso come ARN
GetAccessPoint	Nome del punto di accesso come ARN
ListAccessPoints	Nome del punto di accesso come ARN
PutAccessPointPolicy	Nome del punto di accesso come ARN
GetAccessPointPolicy	Nome del punto di accesso come ARN
DeleteAccessPointPolicy	Nome del punto di accesso come ARN

Creazione e gestione di bucket S3 su Outposts

Per ulteriori informazioni sulla creazione e sulla gestione dei bucket S3 su Outposts, consulta i seguenti argomenti.

Creazione di un bucket S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite

la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

Note

L'Account AWS che crea il bucket lo possiede ed è l'unico che può eseguire azioni su di esso. I bucket dispongono di proprietà di configurazione come Outpost, tag, crittografia di default e impostazioni del punto di accesso. Le impostazioni del punto di accesso includono il Virtual Private Cloud (VPC), la policy del punto di accesso per l'accesso agli oggetti nel bucket e altri metadati. Per ulteriori informazioni, consulta [Specifiche di S3 su Outposts](#).

Se desideri creare un bucket che utilizza AWS PrivateLink per fornire l'accesso alla gestione di bucket ed endpoint tramite endpoint VPC dell'interfaccia nel cloud privato virtuale (VPC), consulta [AWS PrivateLink per S3 su Outposts](#).

Gli esempi seguenti illustrano come creare un bucket S3 su Outposts utilizzando la Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Accedi alla Console di gestione AWS e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona Crea bucket Outposts.
4. In Bucket name (Nome bucket), immettere un nome conforme a DNS (Domain Name System) per il bucket.

Il nome del bucket deve:

- Essere univoco nell'Account AWS, nell'Outpost e nella Regione AWS in cui si trova l'Outpost.
- Contenere da 3 a 63 caratteri.
- Non contiene caratteri maiuscoli.
- Iniziare con una lettera minuscola o un numero.

Una volta creato il bucket, non è possibile modificarne il nome. Per informazioni sulla denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#) nella Guida per l'utente di Amazon S3.

⚠️ Important

Evitare di includere informazioni riservate, ad esempio numeri di account, nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

5. In Outpost, seleziona l'Outpost in cui desideri sia ospitato il bucket.
6. In Bucket Versioning (Controllo delle versioni del bucket), imposta lo stato del controllo delle versioni S3 per il bucket S3 su Outposts su una delle seguenti opzioni:
 - Disable (Disabilita) (impostazione predefinita): il bucket rimane senza versione.
 - Enable (Abilita): il controllo delle versioni S3 è abilitato per gli oggetti nel bucket. A tutti gli oggetti aggiunti al bucket viene assegnato un ID versione univoco.

Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#).

7. (Opzionale) Aggiungi eventuali tag facoltativi che desideri associare al bucket su Outposts. Puoi utilizzare i tag per monitorare i criteri per singoli progetti o gruppi di progetti, o per etichettare i bucket mediante i tag di allocazione dei costi.

Per impostazione predefinita, tutti gli oggetti archiviati nel bucket su Outposts vengono memorizzati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Puoi inoltre scegliere di archiviare esplicitamente gli oggetti utilizzando la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C). Per modificare il tipo di crittografia, è necessario utilizzare l'API REST, AWS Command Line Interface(AWS CLI) oppure gli SDK AWS.

8. Nella sezione Impostazioni punto di accesso Outposts specifica il nome del punto di accesso.

I punti di accesso S3 su Outposts semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in S3 su Outposts. I punti di accesso sono endpoint di rete denominati che vengono collegati a bucket Outposts che puoi usare per eseguire operazioni su oggetti S3. Per ulteriori informazioni, consulta [Access point](#).

I nomi dei punti di accesso devono essere univoci all'interno dell'account per la Regione e l'outpost e devono rispettare le [restrizioni e limitazioni dei punti di accesso](#).

9. Scegli il VPC per questo access point Amazon S3 su Outposts.

Se non hai un VPC scegli Create VPC (Crea VPC). Per ulteriori informazioni, consulta [Creazione di punti di accesso limitati a un cloud privato virtuale \(VPC\)](#) nella Guida per l'utente di Amazon S3.

Un Virtual Private Cloud (VPC) consente di avviare risorse AWS in una rete virtuale definita dall'utente. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'impiego dell'infrastruttura scalabile di AWS.

10. (Facoltativo per un VPC esistente) Scegli una Endpoint subnet (Subnet endpoint) per l'endpoint.

Una sottorete è un intervallo di indirizzi IP nel VPC. Se non disponi della sottorete desiderata, seleziona Crea sottorete. Per ulteriori informazioni, consulta [Reti per S3 su Outposts](#).

11. (Facoltativo per un VPC esistente) Scegli una Endpoint security group (Gruppo di sicurezza endpoint) per l'endpoint.

Un [gruppo di sicurezza](#) agisce da firewall virtuale per controllare il traffico in entrata e in uscita.

12. (Facoltativo per un VPC esistente) Scegli il Endpoint access type (Tipo di accesso all'endpoint):

- Private (Privato): da utilizzare con il VPC.
- Customer owned IP (IP di proprietà del cliente): da utilizzare con un pool di indirizzi IP di proprietà del cliente all'interno della rete On-Premise.

13. (Facoltativo) Specifica la policy del punto di accesso Outpost. La console visualizza automaticamente l'ARN (Amazon Resource Name del punto di accesso che può essere utilizzato nella policy).

14. Seleziona Crea bucket Outposts.

 Note

Per la creazione dell'endpoint per gli outpost e perché il bucket sia pronto all'uso possono essere necessari fino a 5 minuti. Per configurare ulteriori impostazioni di bucket, seleziona Visualizza dettagli.

Utilizzando AWS CLI

Example

L'esempio seguente crea un bucket S3 su Outposts (`s3-outposts:CreateBucket`) utilizzando la AWS CLI. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

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

Utilizzo dell'SDK AWS per Java

Example

Per esempi di come creare un bucket S3 Outposts con il kit AWS SDK per Java, [consulta `CreateOutpostsBucket.java`](#) in Esempi di codice AWS SDK per Java 2.x.

Aggiunta di tag per bucket S3 su Outposts

Puoi aggiungere tag per i bucket Amazon S3 su Outposts per tenere traccia dei costi di storage o di altri criteri per singoli progetti o gruppi di progetti.

Note

L'Account AWS che crea il bucket lo possiede ed è l'unico che ne può cambiare i tag.

Utilizzo della console S3

1. Accedi alla Console di gestione AWS e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts di cui desideri modificare i tag.
4. Scegliere la scheda Properties (Proprietà).
5. In Tags, scegliere Edit (Modifica).

6. Scegli Add new tag (Aggiungi nuovo tag) e completa i campi Key (Chiave) e facoltativamente Value (Valore).

Aggiungi eventuali tag da associare al bucket Outposts per tenere traccia di altri criteri per singoli progetti o gruppi di progetti.

7. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Il seguente esempio AWS CLI applica una configurazione di tag a un bucket S3 su Outposts utilizzando un documento JSON nella cartella corrente che specifica i tag (*tagging.json*). Per utilizzare questo comando, sostituisci *user input placeholder* con le tue informazioni.

```
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"  
    }  
  ]  
}
```

Il seguente esempio AWS CLI applica una configurazione di tag a un bucket S3 su Outposts direttamente dalla riga di 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}]'
```

Per ulteriori informazioni su questo comando, consulta [put-bucket-tagging](#) nella Guida di riferimento di AWS CLI.

Gestione dell'accesso al bucket Amazon S3 su Outposts utilizzando la policy del bucket

Una policy di bucket è una policy AWS Identity and Access Management (IAM) basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni indicate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Le policy di bucket sono limitate a dimensioni di 20 KB. Per ulteriori informazioni, consulta [Policy del bucket](#).

Puoi aggiornare la policy del bucket per gestire l'accesso al bucket Amazon S3 su Outposts. Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

- [Aggiunta o modifica di una policy di un bucket Amazon S3 su Outposts](#)
- [Visualizzazione della policy del bucket Amazon S3 su Outposts](#)
- [Eliminazione della policy del bucket Amazon S3 su Outposts](#)
- [Esempi di policy di bucket](#)

Aggiunta o modifica di una policy di un bucket Amazon S3 su Outposts

Una policy di bucket è una policy AWS Identity and Access Management (IAM) basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni indicate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Le policy di bucket sono limitate a dimensioni di 20 KB. Per ulteriori informazioni, consulta [Policy del bucket](#).

I seguenti argomenti illustrano come aggiornare la policy del bucket Amazon S3 su Outposts utilizzando la Console di gestione AWS, AWS Command Line Interface (AWS CLI) o AWS SDK per Java.

Utilizzo della console S3

Per creare o modificare una policy di bucket

1. Accedi alla Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.

2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts di cui desideri modificare la policy.
4. Scegli la scheda Autorizzazioni.
5. Nella sezione Outposts bucket policy (Policy del bucket Outposts) scegliEdit (Modifica) per creare o modificare la policy.

Ora puoi decidere di aggiungere o modificare la policy del bucket S3 su Outposts. Per ulteriori informazioni, consulta [Configurazione di IAM con S3 su Outposts](#).

Utilizzo di AWS CLI

Nell'esempio della AWS CLI seguente viene inserita una policy su un bucket Outposts.

1. Salva la seguente policy di bucket in un file JSON. In questo esempio, il file è denominato `policy1.json`. Sostituire *user input placeholders* con le proprie informazioni.

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. Inviare il file JSON come parte del comando CLI `put-bucket-policy`. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

```
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
```

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente viene inserita una policy su un bucket 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());  
  
}
```

Visualizzazione della policy del bucket Amazon S3 su Outposts

Una policy di bucket è una policy AWS Identity and Access Management (IAM) basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni indicate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Le policy di bucket sono limitate a dimensioni di 20 KB. Per ulteriori informazioni, consulta [Policy del bucket](#).

I seguenti argomenti illustrano come visualizzare la policy del bucket Amazon S3 su Outposts utilizzando la Console di gestione AWS, AWS Command Line Interface (AWS CLI) o AWS SDK per Java.

Utilizzo della console S3

Per creare o modificare una policy di bucket

1. Accedi alla Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts di cui desideri modificare l'autorizzazione.
4. Scegliere la scheda Permissions (Autorizzazioni).
5. Nella sezione Outposts bucket policy (Policy del bucket Outposts) puoi rivedere la policy del bucket esistente. Per ulteriori informazioni, consulta [Configurazione di IAM con S3 su Outposts](#).

Utilizzo di AWS CLI

Nell'esempio della AWS CLI seguente si ottiene la policy per un bucket di Outposts. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente si ottiene una policy per un bucket 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());  
}
```

Eliminazione della policy del bucket Amazon S3 su Outposts

Una policy di bucket è una policy AWS Identity and Access Management (IAM) basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni indicate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Le policy di bucket sono limitate a dimensioni di 20 KB. Per ulteriori informazioni, consulta [Policy del bucket](#).

I seguenti argomenti illustrano come visualizzare la policy del bucket Amazon S3 su Outposts utilizzando la Console di gestione AWS o AWS Command Line Interface (AWS CLI).

Utilizzo della console S3

Eliminare una policy di bucket

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts di cui desideri modificare l'autorizzazione.
4. Scegliere la scheda Permissions (Autorizzazioni).
5. Nella sezione Policy bucket Outposts, seleziona Elimina.
6. Confermare l'eliminazione.

Utilizzando AWS CLI

Nell'esempio seguente viene eliminata la policy del bucket S3 su Outposts (s3-outposts:DeleteBucket) utilizzando AWS CLI. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

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

Esempi di policy di bucket

Con le policy di bucket S3 su Outposts, è possibile proteggere l'accesso agli oggetti nei bucket S3 su Outposts, in modo che solo gli utenti con le autorizzazioni appropriate possano accedervi. È possibile persino impedire agli utenti autenticati senza le autorizzazioni appropriate di accedere alle risorse S3 su Outposts.

Questa sezione include esempi di casi d'uso tipici per le policy di bucket S3 su Outposts. Per testare queste policy, sostituisci *user input placeholders* con le tue informazioni (come il nome del bucket).

Per concedere o negare le autorizzazioni per un insieme di oggetti, puoi utilizzare caratteri jolly (*) nei nomi delle risorse Amazon (ARN) e altri valori. Ad esempio, puoi controllare l'accesso a gruppi di oggetti che iniziano con un [prefisso](#) comune o terminano con una determinata estensione, come `.html`.

Per informazioni sul linguaggio delle policy AWS Identity and Access Management (IAM), consulta [Configurazione di IAM con S3 su Outposts](#).

Note

Per testare le autorizzazioni [s3outposts](#) utilizzando la console di Amazon S3, è necessario concedere le autorizzazioni aggiuntive richieste dalla console, ovvero `s3outposts:createendpoint`, `s3outposts:listendpoints` e così via.

Risorse aggiuntive per la creazione di policy bucket

- Per un elenco di operazioni, risorse e chiavi di condizione della policy IAM che è possibile utilizzare durante la creazione di una policy bucket S3 su Outposts, consulta [Operazioni, risorse e chiavi di condizione per Amazon S3 su Outposts](#).
- Per istruzioni sulla creazione della policy S3 su Outposts, consulta [Aggiunta o modifica di una policy di un bucket Amazon S3 su Outposts](#).

Argomenti

- [Gestione dell'accesso a un bucket Amazon S3 su Outposts in base a indirizzi IP specifici](#)

Gestione dell'accesso a un bucket Amazon S3 su Outposts in base a indirizzi IP specifici

Una policy di bucket è una policy AWS Identity and Access Management (IAM) basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni indicate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Le policy di bucket sono limitate a dimensioni di 20 KB. Per ulteriori informazioni, consulta [Policy del bucket](#).

Limitare l'accesso a indirizzi IP specifici

L'esempio seguente impedisce a tutti gli utenti di eseguire [operazioni di S3 su Outposts](#) sugli oggetti nei bucket specificati, a meno che la richiesta non provenga dall'intervallo di indirizzi IP specificato.

Note

Quando si limita l'accesso a un indirizzo IP specifico, assicurarsi di specificare anche quali endpoint VPC, indirizzi IP di origine VPC o indirizzi IP esterni possono accedere al bucket S3 su Outposts. In caso contrario, si potrebbe perdere l'accesso al bucket se la policy impedisce a tutti gli utenti sprovvisti delle autorizzazioni appropriate di eseguire operazioni [s3outposts](#) sugli oggetti del bucket S3 su Outposts.

L'istruzione Condition di questa policy identifica **192.0.2.0/24** come l'intervallo di indirizzi IP versione 4 (IPv4) consentiti.

Il blocco Condition utilizza la condizione NotIpAddress e la chiave di condizione aws:SourceIp, che è una chiave di condizione valida per tutto AWS. La chiave di condizione aws:SourceIp può essere utilizzata solo per intervalli di indirizzi IP pubblici. Per ulteriori informazioni sulle chiavi di condizione, consulta [Operazioni, risorse e chiavi di condizione per S3 su Outposts](#). I valori IPv4 aws:SourceIp utilizzano la notazione CIDR standard. Per ulteriori informazioni, consulta [Documentazione di riferimento degli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

⚠ Warning

Prima di utilizzare questa policy S3 su Outposts, sostituire l'intervallo di indirizzi IP **192.0.2.0/24** riportato in questo esempio con un valore appropriato per il proprio caso d'uso. In caso contrario, si perderà la possibilità di accedere al proprio 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"  
        }  
      }  
    }  
  ]  
}
```

Consentire entrambi gli indirizzi IPv4 e IPv6

Quando inizi a utilizzare gli indirizzi IPv6, è consigliabile aggiornare tutte le policy dell'organizzazione con gli intervalli di indirizzi IPv6 in aggiunta agli intervalli di indirizzi IPv4 esistenti. Ciò contribuirà a garantire che le policy continuino a funzionare durante la transizione a IPv6.

Nella policy del bucket S3 su Outposts di esempio seguente viene mostrato come combinare gli intervalli di indirizzi IPv4 e IPv6 per coprire tutti gli indirizzi IP validi dell'organizzazione. La policy di esempio permette l'accesso agli indirizzi IP di esempio **192.0.2.1** e **2001:DB8:1234:5678::1** e lo nega agli indirizzi **203.0.113.1** e **2001:DB8:1234:5678:ABCD::1**.

La chiave di condizione `aws:SourceIp` può essere utilizzata solo per intervalli di indirizzi IP pubblici. I valori IPv6 per `aws:SourceIp` devono essere nel formato CIDR standard. Per IPv6 è supportato l'utilizzo di `::` per rappresentare un intervallo di zeri (0), ad esempio `2001:DB8:1234:5678::/64`. Per ulteriori informazioni, consulta [Operatori di condizione con indirizzo IP](#) nella Guida per l'utente di IAM.

Warning

Sostituire gli intervalli di indirizzi IP in questo esempio con valori appropriati per il proprio caso d'uso prima di utilizzare questa policy S3 su Outposts. In caso contrario, si potrebbe perdere la possibilità di accedere al 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"
        ]
      }
    }
  ]
}
```

Elenco di bucket Amazon S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

Per ulteriori informazioni sull'utilizzo dei bucket in S3 su Outposts, consulta [Utilizzo di bucket S3 su Outposts](#).

Gli esempi seguenti mostrano come ottenere l'elenco dei bucket S3 su Outposts utilizzando Console di gestione AWS, AWS CLI e AWS SDK per Java.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. In Outposts buckets (Bucket Outposts), consulta il tuo elenco di bucket S3 su Outposts.

Utilizzando AWS CLI

L'esempio AWS CLI seguente permette di ottenere un elenco di bucket in un Outpost. Per usare questo comando, sostituire ogni *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [list-regional-buckets](#) nella Guida di riferimento a AWS CLI.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente si ottiene un elenco di bucket in un outpost. Per ulteriori informazioni, consulta [ListRegionalBuckets](#) nella Documentazione di riferimento delle API di 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());  
}
```

Recupero di un bucket S3 su Outposts utilizzando AWS CLI e SDK per Java

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts.

Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

Gli esempi seguenti illustrano come recuperare un bucket S3 su Outposts utilizzando AWS CLI e AWS SDK per Java.

Note

Utilizzando questa operazione con Amazon S3 su Outposts tramite AWS CLI o gli SDK AWS, fornisci l'ARN del punto di accesso per Outposts invece del nome del bucket. Il punto di accesso ARN assume il seguente modulo, dove *region* è il codice Regione AWS per la Regione in cui ha sede Outpost:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Utilizzando AWS CLI

Nell'esempio S3 su Outposts seguente si ottiene un bucket utilizzando AWS CLI. Per usare questo comando, sostituire ogni *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [get-bucket](#) nella Guida di riferimento AWS CLI.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio S3 su Outposts seguente viene ottenuto un bucket utilizzando SDK per Java. Per ulteriori informazioni, consulta la sezione [GetBucket](#) in Guida di riferimento all'API di 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());  
  
}
```

Eliminazione del bucket Amazon S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

Per ulteriori informazioni sull'utilizzo dei bucket in S3 su Outposts, consulta [Utilizzo di bucket S3 su Outposts](#).

L'Account AWS che crea il bucket lo possiede ed è l'unico che può eliminarlo.

Note

- Per poter essere eliminati, i bucket Outposts devono essere vuoti.
La console Amazon S3 non supporta operazioni su oggetti di S3 su Outposts. Per eliminare oggetti nel bucket S3 su Outposts, è necessario utilizzare l'API REST, la AWS CLI o gli SDK AWS.
- Prima di poter eliminare un bucket Outposts, è necessario eliminare tutti i punti di accesso Outposts per il bucket. Per ulteriori informazioni, consulta [Eliminazione di un punto di accesso](#).

- Non è possibile recuperare un bucket dopo che è stato eliminato.

Gli esempi seguenti illustrano come eliminare un bucket S3 su Outposts utilizzando la Console di gestione AWS e AWS Command Line Interface (AWS CLI).

Utilizzo della console S3

1. Accedi alla Console di gestione AWS e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket che desideri eliminare e scegli Elimina.
4. Conferma l'eliminazione.

Utilizzando AWS CLI

L'esempio seguente illustra come eliminare un bucket S3 su Outposts (s3-outposts:DeleteBucket) utilizzando la AWS CLI. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

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

Utilizzo dei punti di accesso Amazon S3 su Outposts

Per accedere al bucket Amazon S3 su Outposts devi creare e configurare un punto di accesso.

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti di Amazon S3, ad esempio GetObject e PutObject. Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. I punti di accesso supportano solo l'indirizzamento in stile hosting virtuale.

Note

L'Account AWS che crea il bucket Outposts lo possiede ed è l'unico che può assegnargli access point.

Nelle sezioni seguenti viene descritto come creare e gestire i punti di accesso per i bucket S3 su Outposts.

Argomenti

- [Creazione di un punto di accesso S3 su Outposts](#)
- [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#)
- [Visualizzazione delle informazioni sulla configurazione di un punto di accesso](#)
- [Visualizzazione dell'elenco dei punti di accesso Amazon S3 su Outposts](#)
- [Eliminazione di un punto di accesso](#)
- [Aggiunta o modifica di una policy del punto di accesso](#)
- [Visualizzazione della policy per un punto di accesso S3 su Outposts](#)

Creazione di un punto di accesso S3 su Outposts

Per accedere al bucket Amazon S3 su Outposts devi creare e configurare un punto di accesso.

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti di Amazon S3, ad esempio GetObject e PutObject. Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. I punti di accesso supportano solo l'indirizzamento in stile hosting virtuale.

Gli esempi seguenti illustrano come creare un punto di accesso per S3 su Outposts utilizzando la Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Note

L'Account AWS che crea il bucket Outposts lo possiede ed è l'unico che può assegnargli access point.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts per il quale desideri creare un punto di accesso Outposts.
4. Seleziona la scheda Punti di accesso Outposts.
5. Nella sezione Punti di accesso Outposts, seleziona Crea punto di accesso Outposts.
6. Nella sezione Outposts access point settings (Impostazioni punto di accesso Outposts), specifica il nome del punto di accesso e quindi seleziona il cloud privato virtuale (VPC) per il punto di accesso.
7. Se desideri aggiungere una policy per il punto di accesso, inseriscila nella sezione Policy punto di accesso Outposts.

Per ulteriori informazioni, consulta [Configurazione di IAM con S3 su Outposts](#).

Utilizzo di AWS CLI

Example

Nell'esempio della AWS CLI seguente viene creato un punto di accesso per un bucket di Outposts. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
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
```

Utilizzo dell'SDK AWS per Java

Example

Per esempi di come creare un punto di accesso per un bucket S3 Outposts con il kit AWS SDK per Java, consulta [CreateOutpostsAccessPoint.java](#) in Esempi di codice SDK AWS per Java 2.x.

Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts

Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. Ogni volta che crei un punto di accesso per un bucket, S3 su Outposts genera automaticamente un alias per tale punto di accesso. Puoi utilizzare questo alias del punto di accesso al posto dell'ARN del punto di accesso per qualsiasi operazione del piano dati. Ad esempio, è possibile utilizzare un alias del punto di accesso per eseguire operazioni a livello di oggetto come PUT, GET, LIST e altre ancora. Per un elenco di queste operazioni, consulta [Operazioni API Amazon S3 per la gestione degli oggetti](#).

Negli esempi seguenti viene illustrato un ARN e un alias per un punto di accesso denominato *my-access-point*.

- ARN del punto di accesso - `arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/my-access-point`
- Alias del punto di accesso - `my-access-po-001ac5d28a6a232904e8xz5w8ijx1qz1bp3i3kuse10--op-s3`

Per ulteriori informazioni sull'utilizzo degli ARN, consulta [Amazon Resource Name \(ARN\)](#) nella Riferimenti generali di AWS.

Per ulteriori informazioni sugli alias del punto di accesso, consulta gli argomenti indicati di seguito.

Argomenti

- [Alias del punto di accesso](#)
- [Utilizzo di un alias del punto di accesso in un'operazione di oggetto S3 su Outposts](#)
- [Restrizioni](#)

Alias del punto di accesso

Un alias del punto di accesso viene creato nello stesso spazio dei nomi del bucket S3 su Outposts. Quando crei un punto di accesso, S3 su Outposts genera automaticamente un alias per tale punto di accesso che non può essere modificato. Un alias del punto di accesso soddisfa tutti i requisiti di un nome di bucket S3 su Outposts valido e comprende le seguenti parti:

access point name prefix-metadata--op-s3

 Note

Il suffisso `--op-s3` è riservato agli alias del punto di accesso; ti consigliamo di non utilizzarlo per i nomi dei bucket o dei punti di accesso. Per ulteriori informazioni sulle regole di denominazione dei bucket S3 su Outposts, consulta [Utilizzo di bucket S3 su Outposts](#).

Ricerca dell'alias del punto di accesso

Negli esempi seguenti viene illustrato come trovare un alias del punto di accesso utilizzando la console Amazon S3 e AWS CLI.

Example - Ricerca e copia dell'alias del punto di accesso nella console Amazon S3

Dopo aver creato un punto di accesso nella console, puoi recuperarne l'alias nella colonna Access Point alias (Alias del punto di accesso) nell'elenco Access Points (Punti di accesso).

Copia dell'alias del punto di accesso

1. Aprire la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. Per copiare l'alias del punto di accesso, effettua una delle seguenti operazioni:
 - Nell'elenco Access Points (Punti di accesso), seleziona il pulsante di opzione accanto al nome del punto di accesso, quindi scegli Copy Access Point alias (Copia alias del punto di accesso).
 - Scegliere il nome del punto di accesso. Quindi, in Outposts access point overview (Panoramica dei punti di accesso Outposts), copia l'alias del punto di accesso.

Example - Creazione di un punto di accesso utilizzando la AWS CLI e ricerca dell'alias del punto di accesso nella risposta

Il seguente esempio del comando `create-access-point` nella AWS CLI crea il punto di accesso e restituisce l'alias del punto di accesso generato automaticamente. Per eseguire questo comando, sostituire `user input placeholders` con le proprie informazioni.

```
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-001ac5d28a6a232904e8xz5w8ijx1qzlpb3i3kuse10--op-s3"
}
```

Example - Recupero di un alias del punto di accesso utilizzando la AWS CLI

L'esempio AWS CLI seguente del comando get-access-point restituisce le informazioni sul punto di accesso specificato. Queste informazioni includono l'alias del punto di accesso. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

```
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": {
    "BlockPublicAccls": true,
    "IgnorePublicAccls": true,
    "BlockPublicPolicy": true,
    "RestrictPublicBuckets": true
  },
  "CreationDate": "2022-09-18T17:49:15.584000+00:00",
  "Alias": "example-outp-00b1d075431d83bebde8xz5w8ijx1qzlpb3i3kuse10--op-s3"
}
```

Example - Elenco dei punti di accesso per trovare un alias del punto di accesso utilizzando la AWS CLI

Il seguente esempio del comando `list-access-points` nella AWS CLI elenca le informazioni sul punto di accesso specificato. Queste informazioni includono l'alias del punto di accesso. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

```
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-00b1d075431d83bebde8xz5w8ijx1qz1bp3i3kuse10--op-s3"
    }
  ]
}
```

Utilizzo di un alias del punto di accesso in un'operazione di oggetto S3 su Outposts

Quando si adottano i punti di accesso, è possibile utilizzare l'alias del punto di accesso senza richiedere importanti modifiche di codice.

Questo esempio nella AWS CLI mostra un'operazione `get-object` per un bucket S3 su Outposts. Questo esempio utilizza l'alias del punto di accesso come valore per `--bucket` anziché l'ARN completo del punto di accesso.

```
aws s3api get-object --bucket my-access-po-
00b1d075431d83bebde8xz5w8ijx1qz1bp3i3kuse10--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": {}
}
```

Restrizioni

- Gli alias non possono essere configurati dai clienti.
- Gli alias non possono essere eliminati, modificati o disabilitati in un punto di accesso.
- Non puoi utilizzare un alias del punto di accesso per le operazioni del piano di controllo (control-plane) S3 su Outposts. Per l'elenco delle operazioni del piano di controllo (control-plane) S3 su Outposts, consulta [Operazioni API Amazon S3 Control per la gestione dei bucket](#).
- Gli alias non possono essere utilizzati nelle policy AWS Identity and Access Management (IAM).

Visualizzazione delle informazioni sulla configurazione di un punto di accesso

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti di Amazon S3, ad esempio `GetObject` e `PutObject`. Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. I punti di accesso supportano solo l'indirizzamento in stile hosting virtuale.

Gli argomenti seguenti descrivono come ottenere le informazioni della configurazione di un punto di accesso Amazon S3 su Outposts utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. Scegli il punto di accesso Outposts per cui desideri visualizzare i dettagli di configurazione.

4. In Outposts access point overview (Panoramica del punto di accesso Outposts), esamina i dettagli della configurazione del punto di accesso.

Utilizzando AWS CLI

Nell'esempio della AWS CLI seguente si ottiene un punto di accesso per un bucket di Outposts. Sostituire *user input placeholders* con le proprie informazioni.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente si ottiene un punto di accesso per un bucket 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());  
  
}
```

Visualizzazione dell'elenco dei punti di accesso Amazon S3 su Outposts

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti di Amazon S3, ad esempio GetObject e PutObject. Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. I punti di accesso supportano solo l'indirizzamento in stile hosting virtuale.

Gli argomenti seguenti descrivono come ottenere l'elenco dei punti di accesso Amazon S3 su Outposts utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. In Outposts access points (Punti di accesso Outposts), consulta l'elenco dei punti di accesso S3 su Outposts.

Utilizzando AWS CLI

Nell'esempio della AWS CLI seguente vengono elencati i punti di accesso per un bucket di Outposts. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente vengono elencati i punti di accesso per un bucket 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());  
  
}
```

Eliminazione di un punto di accesso

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti di Amazon S3, ad esempio GetObject e

PutObject. Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. I punti di accesso supportano solo l'indirizzamento in stile hosting virtuale.

Gli esempi seguenti illustrano come eliminare un punto di accesso utilizzando la Console di gestione AWS e la AWS Command Line Interface (AWS CLI).

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. Nella sezione Punti di accesso Outposts, seleziona il punto di accesso Outposts da eliminare.
4. Scegliere Delete (Elimina).
5. Conferma l'eliminazione.

Utilizzando AWS CLI

Il seguente esempio di AWS CLI mostra come eliminare un punto di accesso su Outposts. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

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

Aggiunta o modifica di una policy del punto di accesso

Ogni punto di accesso dispone di autorizzazioni e controlli di rete distinti che Amazon S3 su Outposts applica per qualsiasi richiesta effettuata tramite il punto di accesso. Ogni punto di accesso applica una policy personalizzata che funziona insieme alla policy di bucket collegata al bucket sottostante. Per ulteriori informazioni, consulta [Access point](#).

Nei seguenti argomenti viene descritto come aggiungere o modificare la policy del punto di accesso per Amazon S3 su Outposts utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).

3. Seleziona il bucket Outposts per il quale desideri modificare la policy del punto di accesso.
4. Seleziona la scheda Punti di accesso Outposts.
5. Nella sezione Punti di accesso Outposts, seleziona il punto di accesso di cui desideri modificare la policy e scegli Modifica policy.
6. Aggiungi o modifica la policy nella sezione Policy punto di accesso Outposts . Per ulteriori informazioni, consulta [Configurazione di IAM con S3 su Outposts](#).

Utilizzo di AWS CLI

Nell'esempio della AWS CLI seguente viene inserita una policy su un punto di accesso Outposts.

1. Salvare la seguente policy del punto di accesso in un file JSON. In questo esempio, il file è denominato `appolicy1.json`. Sostituire *user input placeholders* con le proprie informazioni.

```
{  
  "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. Inviare il file JSON come parte del comando CLI `put-access-point-policy`. Sostituire *user input placeholders* con le proprie informazioni.

```
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
```

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente viene inserita una policy su un punto di accesso 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());  
  
}
```

Visualizzazione della policy per un punto di accesso S3 su Outposts

Ogni punto di accesso dispone di autorizzazioni e controlli di rete distinti che Amazon S3 su Outposts applica a qualsiasi richiesta effettuata tramite il punto di accesso. Ogni punto di accesso applica una policy personalizzata che funziona insieme alla policy di bucket collegata al bucket sottostante. Per ulteriori informazioni, consulta [Access point](#).

Per ulteriori informazioni sull'utilizzo dei punti di accesso in S3 su Outposts, consulta [Utilizzo di bucket S3 su Outposts](#).

Nei seguenti argomenti viene descritto come visualizzare la policy del punto di accesso di Amazon S3 su Outposts utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. Seleziona il punto di accesso Outposts per il quale desideri visualizzare la policy.
4. Nella scheda Permissions (Autorizzazioni) esamina la policy del punto di accesso S3 su Outposts.
5. Per modificare la policy del punto di accesso, consulta [Aggiunta o modifica di una policy del punto di accesso](#).

Utilizzando AWS CLI

Nell'esempio della AWS CLI seguente viene ottenuta una policy per un punto di accesso Outposts. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente si ottiene una policy per un punto di accesso di 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.print("GetAccessPointPolicy Response: %s%n",  
    respGetAccessPointPolicy.toString());  
}
```

}

Utilizzo degli endpoint Amazon S3 su Outposts

Per instradare le richieste verso un punto di accesso Amazon S3 su Outposts, è necessario creare e configurare un endpoint S3 su Outposts. Per creare un endpoint, è necessario disporre di una connessione attiva con il collegamento del servizio alla regione di origine degli outpost. Ogni cloud privato virtuale (VPC) del tuo Outpost può avere un endpoint associato. Per ulteriori informazioni sull'endpoint, consulta [Requisiti di rete di S3 su Outposts](#). È necessario creare un endpoint per poter accedere ai bucket Outposts ed eseguire operazioni sugli oggetti. Per ulteriori informazioni, consulta [Endpoint](#).

Dopo aver creato un endpoint, puoi utilizzare il campo 'Stato' per informazioni sullo stato corrente dell'endpoint. Se gli outpost sono offline, verrà restituito il valore CREATE_FAILED. È possibile verificare la connessione del collegamento del servizio, eliminare l'endpoint e riprovare l'operazione di creazione dopo avere ristabilito la connessione. Per un elenco dei codici di errore aggiuntivi, vedi più avanti. Per ulteriori informazioni, consulta [Endpoint](#).

API	Stato	Codice di errore del motivo dell'operazione non riuscita	Messaggio - Motivo dell'operazione non riuscita
CreateEndpoint	Create_Failed	OutpostNotReachable	Impossibile creare l'endpoint perché la connessione del collegamento del servizio alla regione principale degli outpost è inattiva. Controlla la connessione, elimina l'endpoint e riprova.
CreateEndpoint	Create_Failed	InternalError	Impossibile creare l'endpoint a causa di un errore interno. Elimina l'endpoint e crealo di nuovo.
DeleteEndpoint	Delete_Failed	OutpostNotReachable	Impossibile eliminare l'endpoint perché la connessione del collegamento del servizio alla regione principale degli outpost è inattiva. Controlla la connessione e riprova.

API	Stato	Codice di errore del motivo dell'operazione non riuscita	Messaggio - Motivo dell'operazione non riuscita
DeleteEndpoint	Delete_Failed	InternalError	Impossibile eliminare l'endpoint a causa di un errore interno. Riprova.

Per ulteriori informazioni sull'utilizzo dei bucket in S3 su Outposts, consulta [Utilizzo di bucket S3 su Outposts](#).

Le seguenti sezioni descrivono come creare e gestire gli endpoint per S3 su Outposts.

Argomenti

- [Creazione di un endpoint in un Outpost](#)
- [Visualizzazione dell'elenco degli endpoint Amazon S3 su Outposts](#)
- [Eliminazione di un endpoint Amazon S3 su Outposts](#)

Creazione di un endpoint in un Outpost

Per instradare le richieste verso un punto di accesso Amazon S3 su Outposts, è necessario creare e configurare un endpoint S3 su Outposts. Per creare un endpoint, è necessario disporre di una connessione attiva con il collegamento del servizio alla regione di origine degli outpost. Ogni cloud privato virtuale (VPC) del tuo Outpost può avere un endpoint associato. Per ulteriori informazioni sull'endpoint, consulta [Requisiti di rete di S3 su Outposts](#). È necessario creare un endpoint per poter accedere ai bucket Outposts ed eseguire operazioni sugli oggetti. Per ulteriori informazioni, consulta [Endpoint](#).

Autorizzazioni

Per ulteriori informazioni sulle autorizzazioni richieste per la creazione di un endpoint, consulta [Autorizzazioni per endpoint S3 su Outposts](#).

Quando crei un endpoint, S3 Outposts crea anche un ruolo collegato al servizio nel tuo Account AWS. Per ulteriori informazioni, consulta [Utilizzo dei ruoli collegati ai servizi per Amazon S3 su Outposts](#).

Gli esempi seguenti illustrano come creare un endpoint S3 su Outposts utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Accedi alla Console di gestione AWS e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. Seleziona la scheda Outposts endpoints (Endpoint Outposts).
4. Scegli Create Outposts endpoint (Crea endpoint Outposts).
5. In Outpost, scegli l'Outpost su cui creare questo endpoint.
6. In VPC, scegli un VPC che non disponga ancora di un endpoint e rispetti le regole degli endpoint di Outposts.

Un Virtual Private Cloud (VPC) consente di avviare risorse AWS in una rete virtuale definita dall'utente. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'impiego dell'infrastruttura scalabile di AWS.

Se non si dispone di un VPC, scegliere Crea VPC. Per ulteriori informazioni, consulta [Creazione di punti di accesso limitati a un cloud privato virtuale \(VPC\)](#) nella Guida per l'utente di Amazon S3.

7. Scegli Create Outposts endpoint (Crea endpoint Outposts).

Utilizzando AWS CLI

Example

Nel seguente esempio AWS CLI viene creato un endpoint per un Outpost utilizzando il tipo di accesso alle risorse del VPC. Il VPC deriva dalla sottorete. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

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

Nel seguente esempio AWS CLI viene creato un endpoint per un Outpost utilizzando il tipo di accesso al pool di indirizzi IP di proprietà del cliente (pool CoIP). Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
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
```

Utilizzo dell'SDK AWS per Java

Example

Per esempi su come creare un endpoint per un S3 Outpost con il kit AWS SDK per Java, consulta [CreateOutpostsEndPoint.java](#) in Esempi di codice AWS SDK per Java 2.x.

Visualizzazione dell'elenco degli endpoint Amazon S3 su Outposts

Per instradare le richieste verso un punto di accesso Amazon S3 su Outposts, è necessario creare e configurare un endpoint S3 su Outposts. Per creare un endpoint, è necessario disporre di una connessione attiva con il collegamento del servizio alla regione di origine degli outpost. Ogni cloud privato virtuale (VPC) del tuo Outpost può avere un endpoint associato. Per ulteriori informazioni sull'endpoint, consulta [Requisiti di rete di S3 su Outposts](#). È necessario creare un endpoint per poter accedere ai bucket Outposts ed eseguire operazioni sugli oggetti. Per ulteriori informazioni, consulta [Endpoint](#).

Gli esempi seguenti mostrano come ottenere l'elenco degli endpoint S3 su Outposts utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. Nella pagina Outposts access points (Punti di accesso Outposts) seleziona la scheda Outposts endpoints (Endpoint Outposts).
4. In Outposts endpoints (Endpoint Outposts), puoi visualizzare un elenco dei tuoi endpoint S3 su Outposts.

Utilizzando AWS CLI

Nel seguente esempio AWS CLI sono riportati gli endpoint per le risorse AWS Outposts associate all'account. Per ulteriori informazioni su questo comando, consulta [list-endpoints](#) nella Guida di riferimento a AWS CLI.

```
aws s3outposts list-endpoints
```

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente vengono elencati gli endpoint per un outpost. Per ulteriori informazioni, consulta [ListEndpoints](#) nella Documentazione di riferimento delle API di 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);
}
```

Eliminazione di un endpoint Amazon S3 su Outposts

Per instradare le richieste verso un punto di accesso Amazon S3 su Outposts, è necessario creare e configurare un endpoint S3 su Outposts. Per creare un endpoint, è necessario disporre di una connessione attiva con il collegamento del servizio alla regione di origine degli outpost. Ogni cloud privato virtuale (VPC) del tuo Outpost può avere un endpoint associato. Per ulteriori informazioni sull'endpoint, consulta [Requisiti di rete di S3 su Outposts](#). È necessario creare un endpoint per poter accedere ai bucket Outposts ed eseguire operazioni sugli oggetti. Per ulteriori informazioni, consulta [Endpoint](#).

Gli esempi seguenti mostrano come eliminare gli endpoint S3 su Outposts utilizzando la Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.

2. Nel riquadro di navigazione a sinistra, seleziona Outposts access points (Punti di accesso Outposts).
3. Nella pagina Outposts access points (Punti di accesso Outposts) seleziona la scheda Outposts endpoints (Endpoint Outposts).
4. In Outposts endpoints (Endpoint Outposts) scegli l'endpoint che desideri eliminare e seleziona Delete (Elimina).

Utilizzando AWS CLI

Nell'esempio della AWS CLI seguente viene eliminato un endpoint per un Outpost. Per eseguire questo comando, sostituire *user input placeholders* con le proprie informazioni.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio SDK per Java seguente viene eliminato un endpoint per un Outpost. Per utilizzare questo comando, sostituisci *user input placeholders* con le tue informazioni.

```
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.");
}
```

Utilizzo di oggetti S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST.

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 su Outposts. Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost. Quando specifichi il bucket per le operazioni di oggetto, utilizza il nome della risorsa Amazon (ARN) o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN per i punti di accesso S3 su Outposts, che include il codice Regione AWS per la Regione in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Gli ARN di oggetti utilizzano il seguente formato, che include Regione AWS in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost, il nome del bucket e la chiave dell'oggetto:

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

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

Argomenti

- [Caricare un oggetto in un bucket S3 su Outposts](#)
- [Copia di un oggetto in un bucket Amazon S3 su Outposts utilizzando AWS SDK per Java](#)
- [Recupero di un oggetto da un bucket Amazon S3 su Outposts](#)
- [Elenco di oggetti in un bucket Amazon S3 su Outposts](#)
- [Eliminazione di oggetti nei bucket Amazon S3 su Outposts](#)
- [Utilizzo di HeadBucket per determinare se esiste un bucket S3 su Outposts e sono disponibili le autorizzazioni di accesso](#)
- [Esecuzione e gestione di un caricamento in più parti con SDK per Java](#)
- [Utilizzo di URL prefirmati per S3 su Outposts](#)
- [Amazon S3 su Outposts con Amazon EMR su Outposts locale](#)
- [Memorizzazione nella cache di autorizzazione e autenticazione](#)

Caricare un oggetto in un bucket S3 su Outposts

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 su Outposts. Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost. Quando specifichi il bucket per le operazioni di oggetto, utilizza il nome della risorsa Amazon (ARN) o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN per i punti di accesso S3 su Outposts, che include il codice Regione AWS per la Regione in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

I seguenti esempi AWS CLI e AWS SDK per Java illustrano come caricare un oggetto in un bucket S3 su Outposts utilizzando un punto di accesso.

AWS CLI

Example

Nell'esempio seguente viene inserito un oggetto denominato `sample-object.xml` in un bucket S3 su Outposts (`s3-outposts:PutObject`) utilizzando AWS CLI. Per usare questo comando, sostituisci ogni **user input placeholder** con le informazioni appropriate. Per ulteriori informazioni su questo comando, consulta [put-object](#) nella Guida di riferimento di 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

Per esempi su come caricare un oggetto su un bucket S3 Outposts con il kit AWS SDK per Java, consulta [PutObjectOnOutpost.java](#) in Esempi di codice AWS SDK per Java 2.x.

Copia di un oggetto in un bucket Amazon S3 su Outposts utilizzando AWS SDK per Java

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 su Outposts. Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost. Quando specifichi il bucket per le operazioni di oggetto, utilizza il nome della risorsa Amazon (ARN) o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN per i punti di accesso S3 su Outposts, che include il codice Regione AWS per la Regione in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

L'esempio seguente illustra come copiare un oggetto in un bucket S3 su Outposts utilizzando la AWS SDK per Java.

Utilizzo dell'SDK AWS per Java

Nell'esempio S3 su Outposts seguente un oggetto viene copiato in un nuovo oggetto nello stesso bucket utilizzando l'SDK per Java. Per utilizzare questo comando, sostituisci *user input placeholders* con le tue informazioni.

```
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();
    }
}
```

Recupero di un oggetto da un bucket Amazon S3 su Outposts

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 su Outposts. Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost. Quando specifichi il bucket per le operazioni di oggetto, utilizza il nome della risorsa Amazon (ARN) o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN per i punti di accesso S3 su Outposts, che include il codice Regione AWS per la Regione in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

Gli esempi seguenti illustrano come scaricare un oggetto utilizzando AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzando AWS CLI

Nell'esempio seguente viene inserito un oggetto denominato `sample-object.xml` da un bucket S3 su Outposts (`s3-outposts:GetObject`) utilizzando AWS CLI. Per usare questo comando,

sostituire ogni *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [get-object](#) nella Guida di riferimento a 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
```

Utilizzo dell'SDK AWS per Java

Nell'esempio S3 su Outposts seguente viene ottenuto un oggetto utilizzando SDK per Java. Per utilizzare questo comando, sostituisci *user input placeholder* con le tue informazioni. Per ulteriori informazioni, consulta [GetObject](#) nella Documentazione di riferimento delle API di 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 getObjectContextHeaderOverride = new
GetObjectRequest(accessPointArn, key)
    .withResponseHeaders(headerOverrides);
headerOverrideObject = s3Client.getObject(getObjectContextHeaderOverride);
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();
}
}
```

Elenco di oggetti in un bucket Amazon S3 su Outposts

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 su Outposts. Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost. Quando specifichi il bucket per le operazioni di oggetto, utilizza il nome della risorsa Amazon (ARN) o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN per i punti di accesso S3 su Outposts, che include il codice Regione AWS per la Regione in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Note

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia,

puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

Gli esempi seguenti illustrano come elencare gli oggetti in un bucket S3 su Outposts utilizzando AWS CLI e AWS SDK per Java.

Utilizzando AWS CLI

Nell'esempio seguente sono riportati gli oggetti in un bucket S3 su Outposts (s3-outposts>ListObjectsV2) tramite AWS CLI. Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [list-object-v2](#) nella Guida di riferimento di AWS CLI.

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

Note

Utilizzando questa operazione con Amazon S3 su Outposts tramite le AWS SDK, fornisci l'ARN del punto di accesso Outposts invece del nome del bucket nella seguente scheda: arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-Outposts-Access-Point. Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Utilizzo dell'SDK AWS per Java

Nell'esempio S3 su Outposts seguente vengono elencati oggetti in un bucket utilizzando SDK per Java. Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni.

Important

Questo esempio usa [ListObjectsV2](#), che è l'ultima revisione dell'operazione API ListObjects. Si consiglia di utilizzare questa operazione API rivista per lo sviluppo di applicazioni. Per la compatibilità con le versioni precedenti, Amazon S3 continua a supportare la versione precedente di questa operazione 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();
        }
    }
}
```

Eliminazione di oggetti nei bucket Amazon S3 su Outposts

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 su Outposts. Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost. Quando specifichi il bucket per le operazioni di oggetto, utilizza il nome della risorsa Amazon (ARN) o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN per i punti di accesso S3 su Outposts, che include il codice Regione AWS per la Regione in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

Negli esempi seguenti viene illustrato come eliminare un singolo oggetto o più oggetti in un bucket Amazon S3 su Outposts utilizzando AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzando AWS CLI

Negli esempi seguenti viene illustrato come eliminare un singolo oggetto o più oggetti in un bucket S3 su Outposts.

delete-object

Nell'esempio seguente viene eliminato un oggetto denominato `sample-object.xml` da un bucket S3 su Outposts (`s3-outposts:DeleteObject`) utilizzando AWS CLI. Per eseguire questo comando, sostituire *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [delete-object](#) nella Guida di riferimento 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

Nell'esempio seguente viene eliminato un oggetto denominato `sample-object.xml` e `test1.txt` da un bucket S3 su Outposts (`s3-outposts:DeleteObject`) utilizzando AWS CLI. Per eseguire questo comando, sostituire *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [delete-objects](#) nella Guida di riferimento 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
}
```

}

Utilizzo dell'SDK AWS per Java

Negli esempi seguenti viene illustrato come eliminare un singolo oggetto o più oggetti in un bucket S3 su Outposts.

DeleteObject

Nell'esempio S3 su Outposts seguente viene eliminato un oggetto in un bucket utilizzando SDK per Java. Per utilizzare questo esempio, specificare il punto di accesso ARN per l'Outpost e il nome della chiave dell'oggetto che si desidera eliminare. Per ulteriori informazioni, consulta [DeleteObject](#) nella Documentazione di riferimento delle API di 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

Nell'esempio S3 su Outposts seguente sono caricati e poi eliminati oggetti in un bucket utilizzando SDK per Java. Per utilizzare questo esempio, specificare il punto di accesso ARN per l'Outpost. Per ulteriori informazioni, consulta [DeleteObjects](#) nella Documentazione di riferimento delle API di 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();
}
}
```

Utilizzo di HeadBucket per determinare se esiste un bucket S3 su Outposts e sono disponibili le autorizzazioni di accesso

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 su Outposts. Ogni oggetto è contenuto in un bucket. È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost. Quando specifichi il bucket per le operazioni di oggetto, utilizza il nome della risorsa Amazon (ARN) o l'alias del punto di accesso. Per ulteriori informazioni sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Nell'esempio seguente viene illustrato il formato ARN per i punti di accesso S3 su Outposts, che include il codice Regione AWS per la Regione in cui si trova l'Outpost, l'ID Account AWS, l'ID Outpost e il nome del punto di accesso:

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

Per ulteriori informazioni sugli ARN S3 su Outposts, consulta [ARN delle risorse per S3 su Outposts](#).

Note

Con Amazon S3 su Outposts, i dati degli oggetti vengono sempre archiviati nell'Outpost. Quando AWS installa un rack Outpost, i tuoi dati rimangono locali nel tuo Outpost per soddisfare i requisiti di residenza dei dati. I tuoi oggetti non lasciano mai il tuo Outpost e non sono in una Regione AWS. Dal momento che la Console di gestione AWS è ospitata nella regione, non puoi utilizzare la console per caricare o gestire oggetti nel tuo Outpost. Tuttavia, puoi utilizzare l'API REST, AWS Command Line Interface (AWS CLI) e gli SDK AWS per caricare e gestire gli oggetti tramite i punti di accesso.

I seguenti esempi AWS Command Line Interface (AWS CLI) e AWS SDK per Java illustrano come utilizzare l'operazione API HeadBucket per determinare se esiste un bucket Amazon S3 su Outposts e se sono disponibili le autorizzazioni per accedervi. Per ulteriori informazioni, consulta [HeadBucket](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzando AWS CLI

Nell'esempio AWS CLI di S3 su Outposts seguente viene utilizzato il comando head-bucket per determinare se esiste un bucket e sono disponibili le autorizzazioni per accedervi. Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [head-bucket](#) nella Guida di riferimento di AWS CLI.

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

Utilizzo dell'SDK AWS per Java

Nell'esempio S3 su Outposts seguente viene illustrato come determinare se esiste un bucket e sono disponibili le autorizzazioni per accedervi. Per utilizzare questo esempio, specificare il punto di accesso ARN per l'Outpost. Per ulteriori informazioni, consulta [HeadBucket](#) nella Documentazione di riferimento delle API di 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();
        }
    }
}
```

Esecuzione e gestione di un caricamento in più parti con SDK per Java

Con Amazon S3 su Outposts è possibile creare bucket S3 sulle risorse AWS Outposts, nonché archiviare e recuperare gli oggetti in locale per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

I seguenti esempi mostrano come utilizzare S3 su Outposts con l'AWS SDK per Java per eseguire e gestire un caricamento in più parti.

Argomenti

- [Esecuzione di un caricamento in più parti di un oggetto in un bucket S3 su Outposts](#)
- [Copia di un oggetto in un bucket S3 su Outposts tramite un caricamento in più parti](#)
- [Elencare le parti di un oggetto in un bucket S3 su Outposts](#)
- [Recuperare un elenco di caricamenti in più parti in corso in un bucket S3 su Outposts](#)

Esecuzione di un caricamento in più parti di un oggetto in un bucket S3 su Outposts

L'esempio S3 su Outposts seguente avvia, carica e completa un caricamento in più parti di un oggetto in un bucket utilizzando SDK per Java. Per utilizzare questo esempio, sostituisci *user input placeholder* con le tue informazioni. Per ulteriori informazioni, consulta [Caricamento di un oggetto utilizzando il caricamento in più parti](#) nella Guida per l'utente di 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;
}

```

Copia di un oggetto in un bucket S3 su Outposts tramite un caricamento in più parti

L'esempio seguente S3 su Outposts utilizza SDK per Java per copiare un oggetto in un bucket. Per utilizzare questo esempio, sostituisci *user input placeholder* con le tue informazioni.

```

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;
}
}
```

Elencare le parti di un oggetto in un bucket S3 su Outposts

Nell'esempio S3 su Outposts seguente vengono elencate le parti di un oggetto in un bucket utilizzando SDK per Java. Per utilizzare questo esempio, sostituisci *user input placeholder* con le tue informazioni.

```
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();  
        }  
    }  
}
```

Recuperare un elenco di caricamenti in più parti in corso in un bucket S3 su Outposts

Nell'esempio S3 su Outposts seguente viene illustrato come recuperare un elenco di caricamenti in più parti in corso da un bucket Outposts utilizzando SDK per Java. Per utilizzare questo comando, sostituisci *user input placeholder* con le tue informazioni.

```
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();
    }
}
```

Utilizzo di URL prefirmati per S3 su Outposts

Per concedere un accesso limitato nel tempo agli oggetti memorizzati in locale su un Outpost senza aggiornare la policy del bucket, puoi utilizzare un URL prefirmato. Con gli URL prefirmati, il proprietario del bucket può condividere oggetti con persone nel suo cloud privato virtuale (VPC) o concedere loro la possibilità di caricare o eliminare oggetti.

Quando crei un URL prefirmato utilizzando gli SDK AWS o l'AWS Command Line Interface (AWS CLI), associa l'URL a un'azione specifica. Puoi concedere un accesso limitato nel tempo all'URL prefirmato anche scegliendo una scadenza personalizzata che può essere di appena 1 secondo e fino a 7 giorni. Quando condividi l'URL prefirmato, l'utente del VPC può eseguire l'azione incorporata nell'URL come se fosse l'utente di firma originale. Una volta raggiunta la scadenza, l'URL non funzionerà più.

Limitazione delle funzionalità degli URL prefirmati

Le funzionalità dell'URL prefirmato sono limitate dalle autorizzazioni dell'utente che lo ha creato. In sostanza, gli URL prefirmati sono token di connessione che consentono l'accesso agli utenti che li possiedono. Pertanto, consigliamo di proteggerli in modo appropriato.

AWS Signature Version 4 (SigV4)

Per applicare un comportamento specifico quando le richieste dell'URL prefirmato vengono autenticate tramite AWS Signature Version 4 (SigV4), puoi utilizzare le chiavi di condizione nelle policy del bucket e nelle policy dei punti di accesso. Ad esempio, puoi creare una policy del bucket che utilizzi la condizione `s3-outposts:signatureAge` per negare qualsiasi richiesta di URL

prefirmato da Amazon S3 su Outposts sugli oggetti nel bucket `example-outpost-bucket` se la firma ha più di 10 minuti. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

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": "44445556666"},  
            "Action": "s3-outposts:*",  
            "Resource": "arn:aws:s3-outposts:us-  
east-1:11122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/  
            object/*",  
            "Condition": {  
                "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},  
                "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}  
            }  
        }  
    ]  
}
```

Per un elenco di chiavi di condizione e policy di esempio aggiuntive che è possibile utilizzare per applicare un comportamento specifico quando le richieste dell'URL prefirmato vengono autenticate tramite Signature Version 4, consulta [Chiavi di policy specifiche per l'autenticazione con AWS Signature Version 4 \(SigV4\)](#).

Limitazioni per percorso di rete

Se desideri limitare l'utilizzo di URL prefirmati e tutti gli accessi S3 su Outposts a determinati percorsi di rete, puoi definire policy che richiedono un percorso di rete specifico. Per impostare la restrizione sul principale IAM che effettua la chiamata, puoi utilizzare le policy AWS Identity and Access Management (IAM) basate sull'identità (ad esempio policy di utenti, gruppi o ruoli). Per impostare la restrizione sulla risorsa S3 su Outposts, puoi utilizzare le policy sulle risorse (ad esempio, policy di bucket e punti di accesso).

Una restrizione del percorso di rete sul principale IAM richiede all'utente di tali credenziali di effettuare le richieste dalla rete specificata. Una restrizione sul bucket o sul punto di accesso richiede che tutte le richieste a quella risorsa provengano dalla rete specificata. Queste restrizioni si applicano anche al di fuori dello scenario di URL prefirmato.

La condizione globale IAM utilizzata dipende dal tipo di endpoint. Se utilizzi l'endpoint pubblico per S3 su Outposts, utilizza `aws:SourceIp`. Se utilizzi un endpoint VPC per S3 su Outposts, utilizza `aws:SourceVpc` o `aws:SourceVpce`.

La seguente istruzione di policy IAM richiede che il principale del servizio acceda ad AWS solo dall'intervallo di rete specificato. Con questa istruzione della policy, tutti gli accessi devono avere origine da tale intervallo. Ciò include il caso di un utente che utilizza un URL prefirmato per S3 su Outposts. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

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

Per un esempio di policy del bucket che utilizza la chiave di condizione globale `aws:SourceIP` AWS per limitare l'accesso a un bucket S3 su Outposts a un intervallo di rete specifico, consulta [Configurazione di IAM con S3 su Outposts](#).

Chi può creare un URL prefirmato

Qualsiasi utente che disponga di credenziali di sicurezza valide può creare un URL prefirmato. Tuttavia, perché un utente nel VPC possa accedere a un oggetto, è necessario che l'URL prefirmato venga creato da un utente che dispone dell'autorizzazione a eseguire l'operazione su cui si basa l'URL prefirmato.

Per creare un URL prefirmato puoi utilizzare le seguenti credenziali:

- Profilo dell'istanza IAM: valido fino a 6 ore.

- AWS Security Token Service: valido fino a 36 ore quando viene firmato con credenziali permanenti, ad esempio quelle dell'utente root dell'Account AWS o di un utente IAM.
- Utente IAM: valido fino a 7 giorni quando utilizzi AWS Signature Version 4.

Per creare un URL prefirmato valido fino a 7 giorni, devi prima delegare le credenziali dell'utente IAM (la chiave di accesso e la chiave segreta) all'SDK in uso. Quindi, genera un URL prefirmato utilizzando AWS Signature Version 4.

Note

- Se hai creato un URL prefirmato utilizzando un token temporaneo, l'URL scade insieme al token, anche se per l'URL è indicata una data di scadenza successiva.
- Poiché gli URL prefirmati consentono l'accesso ai tuoi bucket S3 su Outposts a chiunque disponga dell'URL, ti consigliamo di proteggere tali URL in modo appropriato. Per ulteriori informazioni sulla protezione di URL prefirmati, consulta la sezione [Limitazione delle funzionalità degli URL prefirmati](#).

Quando S3 su Outposts verifica la data e l'ora di scadenza in un URL prefirmato?

Al momento della richiesta HTTP, S3 su Outposts controlla la data e l'ora di scadenza di un URL firmato. Ad esempio, se un client inizia a scaricare un file di grandi dimensioni immediatamente prima dell'ora di scadenza, il download viene completato anche se l'ora di scadenza viene superata. Se la connessione TCP viene interrotta e il client prova a riavviare il download dopo la scadenza, il download non riesce.

Per ulteriori informazioni sull'utilizzo di un URL prefirmato per condividere o caricare oggetti, consulta gli argomenti riportati di seguito.

Argomenti

- [Condivisione di oggetti mediante URL prefirmati](#)
- [Generazione di un URL prefirmato per il caricamento di un oggetto in un bucket S3 su Outposts](#)

Condivisione di oggetti mediante URL prefirmati

Per concedere un accesso limitato nel tempo agli oggetti memorizzati in locale su un Outpost senza aggiornare la policy del bucket, puoi utilizzare un URL prefirmato. Con gli URL prefirmati, il proprietario del bucket può condividere oggetti con persone nel suo cloud privato virtuale (VPC) o concedere loro la possibilità di caricare o eliminare oggetti.

Quando crei un URL prefirmato utilizzando gli SDK AWS o l'AWS Command Line Interface (AWS CLI), associa l'URL a un'azione specifica. Puoi concedere un accesso limitato nel tempo all'URL prefirmato anche scegliendo una scadenza personalizzata che può essere di appena 1 secondo e fino a 7 giorni. Quando condividi l'URL prefirmato, l'utente del VPC può eseguire l'azione incorporata nell'URL come se fosse l'utente di firma originale. Una volta raggiunta la scadenza, l'URL non funzionerà più.

Quando crei un URL prefirmato, devi fornire le credenziali di sicurezza e specificare quanto segue:

- Un nome della risorsa Amazon (ARN) del punto di accesso per il bucket S3 su Outposts.
- Una chiave oggetto
- Un metodo HTTP (GET per scaricare gli oggetti)
- Una data e un'ora di scadenza

Un URL prefirmato è valido solo per la durata specificata. In altre parole, è necessario avviare l'operazione consentita dall'URL prima della sua data e ora di scadenza. L'URL prefirmato può essere utilizzato più volte, fino alla data e all'ora di scadenza. Se hai creato un URL prefirmato utilizzando un token temporaneo, l'URL scade insieme al token, anche se per l'URL è indicata una data di scadenza successiva.

Gli utenti nel cloud privato virtuale (VPC) che hanno accesso all'URL prefirmato possono caricare oggetti. Ad esempio, se il bucket contiene un video e sia il bucket che l'oggetto sono privati, è possibile condividere il video con altri generando un URL prefirmato. Poiché gli URL prefirmati consentono l'accesso ai tuoi bucket S3 su Outposts a chiunque disponga dell'URL, ti consigliamo di proteggere tali URL in modo appropriato. Per ulteriori informazioni sulla protezione degli URL prefirmati, consulta [Limitazione delle funzionalità degli URL prefirmati](#).

Qualsiasi utente che disponga di credenziali di sicurezza valide può creare un URL prefirmato. Tuttavia, l'URL prefirmato deve essere creato da un utente dotato dell'autorizzazione per eseguire

l'operazione su cui si basa l'URL. Per ulteriori informazioni, consulta [Chi può creare un URL prefirmato](#).

È possibile generare un URL prefirmato per condividere un oggetto in un bucket S3 su Outposts utilizzando AWSSDK e AWS CLI. Per maggiori informazioni, consulta i seguenti esempi.

Uso degli AWS SDK

Per generare un URL prefirmato che puoi fornire ad altri utenti in modo che questi possano richiamare un oggetto, puoi utilizzare gli SDK AWS.

Note

Quando utilizzi gli SDK AWS per generare un URL prefirmato, il tempo massimo di scadenza per un URL è di 7 giorni dal momento della creazione.

Java

Example

Nel seguente esempio viene generato un URL prefirmato che è possibile fornire ad altri utenti in modo che possano recuperare un oggetto da un bucket S3 su Outposts. Per ulteriori informazioni, consulta [Utilizzo di URL prefirmati per S3 su Outposts](#). Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
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

Nel seguente esempio viene generato un URL prefirmato che è possibile fornire ad altri utenti in modo che possano recuperare un oggetto da un bucket S3 su Outposts. Per ulteriori informazioni,

consulta [Utilizzo di URL prefirmati per S3 su Outposts](#). Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
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

Nel seguente esempio viene generato un URL prefirmito per condividere un oggetto utilizzando l'SDK per Python (Boto3). Ad esempio, utilizza un client Boto3 e la funzione `generate_presigned_url` per generare un URL prefirmito che ti consenta di eseguire il GET di un oggetto.

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

Per ulteriori informazioni sull'utilizzo dell'SDK per Python (Boto3) per generare un URL prefirmito, consulta [Python](#) nella Documentazione di riferimento delle API di AWS SDK per Python (Boto).

Utilizzando AWS CLI

L'esempio seguente AWS CLI command genera un URL prefirmito per un bucket S3 su Outposts. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Note

Quando utilizzi la AWS CLI per generare un URL prefirmito, il tempo massimo di scadenza per un URL è di 7 giorni dal momento della creazione.

```
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
```

Per ulteriori informazioni, consulta [presign](#) nella documentazione di riferimento dei comandi della AWS CLI.

Generazione di un URL prefirmato per il caricamento di un oggetto in un bucket S3 su Outposts

Per concedere un accesso limitato nel tempo agli oggetti memorizzati in locale su un Outpost senza aggiornare la policy del bucket, puoi utilizzare un URL prefirmato. Con gli URL prefirmati, il proprietario del bucket può condividere oggetti con persone nel suo cloud privato virtuale (VPC) o concedere loro la possibilità di caricare o eliminare oggetti.

Quando crei un URL prefirmato utilizzando gli SDK AWS o l'AWS Command Line Interface (AWS CLI), associa l'URL a un'azione specifica. Puoi concedere un accesso limitato nel tempo all'URL prefirmato anche scegliendo una scadenza personalizzata che può essere di appena 1 secondo e fino a 7 giorni. Quando condividi l'URL prefirmato, l'utente del VPC può eseguire l'azione incorporata nell'URL come se fosse l'utente di firma originale. Una volta raggiunta la scadenza, l'URL non funzionerà più.

Quando crei un URL prefirmato, devi fornire le credenziali di sicurezza e specificare quanto segue:

- Un nome della risorsa Amazon (ARN) del punto di accesso per il bucket S3 su Outposts.
- Una chiave oggetto
- Un metodo HTTP (PUT per il caricamento di oggetti)
- Una data e un'ora di scadenza

Un URL prefirmato è valido solo per la durata specificata. In altre parole, è necessario avviare l'operazione consentita dall'URL prima della sua data e ora di scadenza. L'URL prefirmato può essere utilizzato più volte, fino alla data e all'ora di scadenza. Se hai creato un URL prefirmato utilizzando un token temporaneo, l'URL scade insieme al token, anche se per l'URL è indicata una data di scadenza successiva.

Se l'operazione consentita da un URL prefirmato è costituita da più fasi, ad esempio un caricamento in più parti, tutti le fasi devono essere avviate prima della scadenza. Se S3 su Outposts prova ad avviare una fase con un URL scaduto, viene restituito un errore.

Gli utenti nel cloud privato virtuale (VPC) che hanno accesso all'URL prefirmato possono caricare oggetti. Ad esempio, un utente nel VPC che ha accesso all'URL prefirmato può caricare un oggetto nel tuo bucket. Poiché gli URL prefirmati consentono l'accesso ai tuoi bucket S3 su Outposts a qualsiasi utente nel VPC che abbia accesso all'URL prefirmato, ti consigliamo di proteggere tali URL in modo appropriato. Per ulteriori informazioni sulla protezione degli URL prefirmati, consulta [Limitazione delle funzionalità degli URL prefirmati](#).

Qualsiasi utente che disponga di credenziali di sicurezza valide può creare un URL prefirmato. Tuttavia, l'URL prefirmato deve essere creato da un utente dotato dell'autorizzazione per eseguire l'operazione su cui si basa l'URL. Per ulteriori informazioni, consulta [Chi può creare un URL prefirmato](#).

Uso degli SDK AWS per generare un URL prefirmato per un'operazione sugli oggetti S3 su Outpost

Java

SDK per Java 2.x

Questo esempio mostra come generare un URL prefirmato utilizzabile da un bucket S3 su Outposts per un periodo di tempo limitato. Per ulteriori informazioni, consulta [Utilizzo di URL prefirmati per S3 su 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.printStackTrace();
} catch (IOException e) {
e.printStackTrace();
}
}
```

Python

SDK per Python (Boto3)

In questo esempio viene mostrato come generare un URL prefirmato in grado di eseguire un'operazione S3 su Outposts per un periodo di tempo limitato. Per ulteriori informazioni,

consulta [Utilizzo di URL prefirmati per S3 su Outposts](#). Per effettuare una richiesta con l'URL, utilizza il pacchetto 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 su Outposts con Amazon EMR su Outposts locale

Amazon EMR è una piattaforma di cluster gestita che semplifica l'esecuzione di framework di Big Data, come ad esempio Apache Hadoop e Apache Spark su AWS per elaborare e analizzare grandi quantità di dati. Utilizzando questi framework e i relativi progetti open source, è possibile elaborare i dati per scopi di analisi e carichi di lavoro di business intelligence. Amazon EMR consente inoltre di trasformare e spostare grandi quantità di dati all'interno e all'esterno di altri datastore e database AWS e supporta Amazon S3 su Outposts. Per ulteriori informazioni su Amazon EMR, consulta [Amazon EMR su Outposts](#) nella Guida alla gestione di Amazon EMR.

Per Amazon S3 su Outposts, Amazon EMR ha iniziato a supportare il connettore Apache Hadoop S3A nella versione 7.0.0. Le versioni precedenti di Amazon EMR non supportano S3 su Outposts locale e il file system EMR (EMRFS) non è supportato.

Applicazioni supportate

Amazon EMR con Amazon S3 su Outposts supporta le seguenti applicazioni:

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

Per ulteriori informazioni, consulta la [Guida ai rilasci di Amazon EMR](#).

Creare e configurare un bucket Amazon S3 su Outposts

Amazon EMR utilizza AWS SDK per Java con Amazon S3 su Outposts per archiviare dati di input e dati di output. I file di log di Amazon EMR sono archiviati in una posizione Amazon S3 regionale

selezionata e non sono archiviati localmente su Outpost. Per ulteriori informazioni, consulta [Log di Amazon EMR](#) nella Guida alla gestione di Amazon EMR.

Per conformarsi ai requisiti di Amazon S3 e DNS, i bucket S3 su Outposts presentano restrizioni e limitazioni di denominazione. Per ulteriori informazioni, consulta [Creazione di un bucket S3 su Outposts](#).

Con Amazon EMR versione 7.0.0 e successive, è possibile utilizzare Amazon EMR con S3 su Outposts e il file system S3A.

Prerequisiti

Autorizzazioni di S3 su Outposts: quando si crea un profilo dell'istanza Amazon EMR, il ruolo deve contenere lo spazio dei nomi AWS Identity and Access Management (IAM) per S3 su Outposts. S3 su Outposts ha il proprio spazio dei nomi, `s3-outposts`*. Per una policy di esempio che utilizza questo spazio dei nomi, consulta [Configurazione di IAM con S3 su Outposts](#).

Connettore S3A: per configurare il cluster EMR per accedere ai dati da un bucket Amazon S3 su Outposts, è necessario utilizzare il connettore Apache Hadoop S3A. Per utilizzare il connettore, assicurarsi che tutti gli URI S3 utilizzino lo schema `s3a`. In caso contrario, è possibile configurare l'implementazione del file system utilizzata per il cluster EMR in modo che gli URI S3 funzionino con il connettore S3A.

Per configurare l'implementazione del file system in modo che funzioni con il connettore S3A, utilizzare le proprietà di configurazione `fs.file_scheme.impl` e `fs.AbstractFileSystem.file_scheme.impl` per il cluster EMR, dove `file_scheme` corrisponde al tipo di URI S3 di cui si dispone. Per utilizzare l'esempio seguente, sostituisci `user input placeholders` con le informazioni appropriate. Ad esempio, per modificare l'implementazione del file system per gli URI S3 che utilizzano lo schema `s3`, specificare le seguenti proprietà di configurazione del cluster:

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

Per utilizzare S3A, impostare la proprietà di configurazione `fs.file_scheme.impl` su `org.apache.hadoop.fs.s3a.S3AFileSystem` e impostare la proprietà `fs.AbstractFileSystem.file_scheme.impl` su `org.apache.hadoop.fs.s3a.S3A`.

Ad esempio, se si sta accedendo al percorso `s3a://bucket/...`, impostare la proprietà `fs.s3a.impl` su `org.apache.hadoop.fs.s3a.S3AFileSystem` e impostate la proprietà `fs.AbstractFileSystem.s3a.impl` su `org.apache.hadoop.fs.s3a.S3A`.

Nozioni di base sull'uso di Amazon EMR con Amazon S3 su Outposts

Gli argomenti seguenti spiegano come iniziare a utilizzare Amazon EMR con Amazon S3 su Outposts.

Argomenti

- [Creazione di una policy di autorizzazione](#)
- [Creazione e configurazione del cluster](#)
- [Panoramica delle configurazioni](#)
- [Considerazioni](#)

Creazione di una policy di autorizzazione

Per poter creare un cluster EMR che utilizza Amazon S3 su Outposts, è necessario creare una policy IAM da collegare al profilo dell'istanza Amazon EC2 per il cluster. La policy deve disporre delle autorizzazioni per accedere al nome della risorsa Amazon (ARN) del punto di accesso S3 su Outposts. Per ulteriori informazioni sulla creazione di policy IAM per S3 su Outposts, consulta [Configurazione di IAM con S3 su Outposts](#).

La policy di esempio seguente mostra come concedere le autorizzazioni richieste. Dopo avere creato la policy, collegala al ruolo del profilo dell'istanza utilizzato per creare il cluster EMR, come descritto nella sezione [the section called “Creazione e configurazione del cluster”](#). Per utilizzare questo esempio, sostituisci `user input placeholders` con le informazioni appropriate.

```
{  
  "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:*"  
  ]  
}  
}  
}
```

Creazione e configurazione del cluster

Per creare un cluster che esegua Spark con S3 su Outposts, completare i seguenti passaggi nella console.

Per creare un cluster che esegua Spark con S3 su Outposts

1. Apri la console di Amazon EMR all'indirizzo <https://console.aws.amazon.com/elasticmapreduce/>.
 2. Nel pannello di navigazione a sinistra, seleziona Cluster.
 3. Scegliere Crea cluster.
-
4. Per la versione di Amazon EMR, scegli emr-7.0.0 o versione successiva.
 5. Per il bundle di applicazioni, scegli Spark interattivo. Seleziona quindi tutte le altre applicazioni supportate che desideri includere nel cluster.
 6. Per abilitare Amazon S3 su Outposts, immettere le impostazioni di configurazione.

Impostazioni di configurazione di esempio

Per utilizzare le impostazioni di configurazione di esempio seguenti, sostituisci *user input placeholders* con le informazioni appropriate.

```
[  
 {  
   "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. Nella sezione Rete, scegli un cloud privato virtuale (VPC) e una sottorete che si trovano nel rack AWS Outposts. Per ulteriori informazioni su Amazon EMR su Outposts, consulta [Cluster EMR su AWS Outposts](#) nella Guida alla gestione di Amazon EMR.
8. Nella sezione Profilo dell'istanza EC2 per Amazon EMR, scegli il ruolo IAM a cui è allegata la [policy di autorizzazione creata in precedenza](#).

9. Configura le impostazioni rimanenti del cluster, quindi scegli Crea cluster.

Panoramica delle configurazioni

La tabella seguente descrive le configurazioni S3A e i valori da specificare per i relativi parametri quando si configura un cluster che utilizza S3 su Outposts con Amazon EMR.

Parametro	Valore predefinito	Valore richiesto per S3 su Outposts	Spiegazione
<code>fs.s3a.aws.credentials.provider</code>	Se non specificato, S3A cercherà S3 nel bucket Regione con il nome del bucket Outposts.	ARN del punto di accesso del bucket S3 su Outposts	Amazon S3 su Outposts supporta i punti di accesso configurati solo per i virtual private cloud (VPC) come unico mezzo per accedere ai bucket di Outposts.
<code>fs.s3a.committer.name</code>	<code>file</code>	<code>magic</code>	Il committer <code>magic</code> è l'unico committer supportato per S3 su Outposts.
<code>fs.s3a.select.enabled</code>	<code>TRUE</code>	<code>FALSE</code>	S3 Select non è supportato su Outposts.
<code>JAVA_HOME</code>	<code>/usr/lib/jvm/java-8</code>	<code>/usr/lib/jvm/java-11-amazon-corretto.x86_64</code>	S3 su Outposts su S3A richiede Java versione 11.

La tabella seguente descrive le configurazioni Spark e i valori da specificare per i relativi parametri quando si configura un cluster che utilizza S3 su Outposts con Amazon EMR.

Parametro	Valore predefinito	Valore richiesto per S3 su Outposts	Spiegazione
spark.sql.sources.fastS3PartitionDiscovery.enabled	TRUE	FALSE	S3 su Outposts non supporta la partizione veloce.
spark.executorEnv.JAVA_HOME	/usr/lib/jvm/java-8	/usr/lib/jvm/java-11-amazon-corretto.x86_64	S3 su Outposts su S3A richiede Java versione 11.

Considerazioni

Quando si integra Amazon EMR con i bucket S3 su Outposts, tenere presente quanto segue:

- Amazon S3 su Outposts è supportato con Amazon EMR versione 7.0.0 e successive.
- Il connettore S3A è necessario per utilizzare S3 su Outposts con Amazon EMR. Solo S3A dispone delle funzionalità necessarie per interagire con i bucket S3 su Outposts. Per informazioni sulla configurazione del connettore S3A, consulta la sezione [Prerequisiti](#).
- Amazon S3 su Outposts supporta solo la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) con Amazon EMR. Per ulteriori informazioni, consulta [the section called “Crittografia dei dati”](#).
- Amazon S3 su Outposts non supporta le scritture con S3A FileOutputStreamCommitter. Le scritture con S3A FileOutputStreamCommitter su S3 sui bucket Outposts generano il seguente errore: InvalidStorageClass: La classe di storage specificata non è valida.
- Amazon S3 su Outposts non è supportato con Amazon EMR serverless o Amazon EMR su EKS.
- I log di Amazon EMR sono archiviati in una posizione Amazon S3 regionale selezionata e non sono archiviati localmente nel bucket S3 su Outposts.

Memorizzazione nella cache di autorizzazione e autenticazione

S3 su Outposts memorizza nella cache in modo sicuro i dati di autenticazione e autorizzazione localmente nei rack Outposts. La cache rimuove i round trip verso la Regione AWS principale per ogni richiesta. In questo modo si elimina la variabilità introdotta dai round trip della rete. Con la cache di autenticazione e autorizzazione di S3 su Outposts, si ottengono latenze coerenti indipendenti dalla latenza della connessione tra Outposts e la Regione AWS.

Quando si effettua una richiesta API S3 su Outposts, i dati di autenticazione e autorizzazione vengono memorizzati nella cache in modo sicuro. I dati memorizzati nella cache vengono quindi utilizzati per autenticare le successive richieste API degli oggetti S3. S3 su Outposts memorizza nella cache i dati di autenticazione e autorizzazione solo quando la richiesta viene firmata utilizzando Signature Version 4A (SigV4A). La cache viene archiviata localmente sugli Outposts all'interno del servizio S3 su Outposts. Viene aggiornata in modo asincrono quando si effettua una richiesta API S3. La cache è crittografata e sugli Outposts non viene archiviata alcuna chiave crittografica in testo normale.

La cache è valida per un massimo di 10 minuti quando l'Outpost è connesso alla Regione AWS. Viene aggiornata in modo asincrono quando si effettua una richiesta API S3 su Outposts, per garantire l'utilizzo delle policy più recenti. Se l'Outpost viene disconnesso dalla Regione AWS, la cache sarà valida per un massimo di 12 ore.

Configurazione della cache di autorizzazione e autenticazione

S3 su Outposts memorizza automaticamente nella cache i dati di autenticazione e autorizzazione per le richieste firmate con l'algoritmo SigV4A. Per ulteriori informazioni, consulta [Firma delle richieste API AWS](#) nella AWS Identity and Access Management Guida per l'utente di . L'algoritmo SigV4A è disponibile nelle ultime versioni degli SDK AWS. È possibile ottenerlo tramite una dipendenza dalle librerie [AWS Common Runtime \(CRT\)](#).

È necessario utilizzare la versione più recente dell'SDK AWS e installare la versione più recente del CRT. Ad esempio, è possibile eseguire `pip install awscrt` per ottenere la versione più recente del CRT con Boto3.

S3 su Outposts non memorizza automaticamente nella cache i dati di autenticazione e autorizzazione per le richieste firmate con l'algoritmo SigV4.

Convalida della firma SigV4A

È possibile utilizzare AWS CloudTrail per verificare che le richieste siano state firmate con SigV4A. Per ulteriori informazioni sulla configurazione di CloudTrail per S3 su Outposts, consulta [Monitoraggio di S3 su Outposts con i log AWS CloudTrail](#).

Dopo aver configurato CloudTrail, è possibile verificare come è stata firmata una richiesta nel campo `SignatureVersion` dei log di CloudTrail. Le richieste firmate con SigV4A avranno `SignatureVersion` impostato su `AWS4-ECDSA-P256-SHA256`. Le richieste firmate con SigV4 avranno `SignatureVersion` impostato su `AWS4-HMAC-SHA256`.

Sicurezza in S3 su Outposts

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue Servizi AWS nel Cloud AWS. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei [Programmi di conformità AWS](#). Per informazioni sui programmi di conformità applicabili ad Amazon S3 su Outposts, consulta [Servizi AWS coperti dal programma di conformità](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal Servizio AWS che viene utilizzato. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione illustra come applicare il modello di responsabilità condivisa quando si usa S3 su Outposts. I seguenti argomenti illustrano come configurare S3 su Outposts per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri servizi Servizi AWS per monitorare e proteggere le risorse S3 su Outposts.

Argomenti

- [Configurazione di IAM con S3 su Outposts](#)
- [Crittografia dei dati in S3 su Outposts](#)
- [AWS PrivateLink per S3 su Outposts](#)
- [Chiavi di policy specifiche per l'autenticazione con AWS Signature Version 4 \(SigV4\)](#)
- [Policy gestite da AWS per Amazon S3 su Outposts](#)
- [Utilizzo dei ruoli collegati ai servizi per Amazon S3 su Outposts](#)

Configurazione di IAM con S3 su Outposts

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può

autenticarsi (eseguire l'accesso) ed è autorizzato (dispone di autorizzazioni) a utilizzare le risorse di Amazon S3 su Outpost. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi. Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per le risorse e le operazioni di S3 su Outposts. Per concedere le autorizzazioni di accesso per S3 sulle risorse e le operazioni API di Outposts, puoi utilizzare IAM per creare [utenti](#), [gruppi](#) o [ruoli](#) a cui associare le autorizzazioni.

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Create a role for a third-party identity provider \(federation\)](#) della Guida per l'utente IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina [Create a role for an IAM user](#) della Guida per l'utente IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente IAM.

Oltre alle policy IAM basate sull'identità, S3 su Outposts supporta sia le policy del bucket che le policy dei punti di accesso. Le policy del bucket e le policy del punto di accesso sono [policy basate sulle risorse](#) collegate alla risorsa S3 su Outposts.

- Una policy del bucket è collegata al bucket e consente o nega le richieste al bucket e agli oggetti in esso contenuti in base agli elementi nella policy.
- Al contrario, una policy del punto di accesso è collegata al punto di accesso e consente o nega le richieste al punto di accesso.

La policy del punto di accesso funziona con la policy del bucket collegata al bucket S3 su Outposts sottostante. Affinché un'applicazione o un utente possa accedere agli oggetti in un bucket S3 su Outposts tramite un punto di accesso S3 su Outposts, sia la policy del punto di accesso che la policy del bucket devono consentire la richiesta.

Le limitazioni incluse in una policy di access point si applicano solo alle richieste effettuate tramite quell'access point. Ad esempio, se un punto di accesso è collegato a un bucket, non potrai utilizzare la policy del punto di accesso per consentire o negare le richieste che vengono effettuate direttamente al bucket. Tuttavia, le restrizioni applicate a una policy del bucket possono consentire o rifiutare le richieste effettuate direttamente al bucket o tramite il punto di accesso.

In una policy IAM o in una policy basata su risorse, definisci quali operazioni S3 su Outposts saranno consentite o negate. Le operazioni S3 su Outposts corrispondono a operazioni API S3 su Outposts specifiche. Le operazioni S3 su Outposts utilizzano il prefisso dello spazio dei nomi `s3-outposts:`. Le richieste effettuate all'API di controllo S3 su Outposts in Regione AWS e le richieste effettuate agli endpoint dell'API dell'oggetto sull'Outpost vengono autenticate utilizzando IAM e sono autorizzate rispetto al prefisso dello spazio dei nomi `s3-outposts:`. Configurare gli utenti IAM e autorizzarli a fronte dello spazio dei nomi IAM `s3-outposts:` per lavorare con S3 su Outposts.

Per ulteriori informazioni, consulta [Operazioni, risorse e chiavi di condizione per Amazon S3 su Outposts](#) nella Documentazione di riferimento per l'autorizzazione ai servizi.

Note

- Le liste di controllo degli accessi (ACL) non sono supportate in S3 su Outposts.
- Per impostazione predefinita, S3 su Outposts definisce il proprietario del bucket come proprietario dell'oggetto per avere la certezza che al proprietario di un bucket non possa essere impedito di accedere o eliminare oggetti.
- S3 su Outposts dispone sempre di accesso pubblico blocco S3 abilitato per garantire che gli oggetti non possano mai avere accesso pubblico.

Per ulteriori informazioni sulla configurazione di IAM per S3 su Outposts, consulta i seguenti argomenti.

Argomenti

- [Principi per le policy di S3 su Outposts](#)
- [ARN delle risorse per S3 su Outposts](#)
- [Esempi di policy per S3 su Outposts](#)
- [Autorizzazioni per endpoint S3 su Outposts](#)
- [Ruoli collegati ai servizi per S3 su Outposts](#)

Principi per le policy di S3 su Outposts

Quando crei una policy basata su risorse per concedere l'accesso al bucket S3 su Outposts, devi utilizzare l'elemento `Principal` per specificare la persona o l'applicazione che può effettuare una richiesta per un'azione o un'operazione su tale risorsa. Per le policy S3 su Outposts, puoi utilizzare uno dei seguenti principali:

- Un Account AWS
- Un utente IAM
- Un ruolo IAM:
- Tutti i principali, specificando un carattere jolly (*) in una policy che utilizza un elemento `Condition` per limitare l'accesso a un intervallo IP specifico

Important

Non puoi scrivere una policy per un bucket S3 su Outposts che utilizza un carattere jolly (*) nell'elemento `Principal` a meno che la policy non includa anche una `Condition` che limita l'accesso a un intervallo di indirizzi IP specifico. Questa limitazione garantisce che non vi sia alcun accesso pubblico al bucket S3 su Outposts. Per vedere un esempio, consulta [Esempi di policy per S3 su Outposts](#).

Per ulteriori informazioni sull'elemento `Principal`, consulta [Elementi della policy JSON di AWS: principale](#) nella Guida per l'utente di IAM.

ARN delle risorse per S3 su Outposts

Gli Amazon Resource Name (ARN) per S3 su Outposts contengono l'ID Outpost oltre a Regione AWS, ID Account AWS e nome della risorsa. Per accedere ed eseguire operazioni sui bucket e sugli oggetti Outposts, è necessario utilizzare uno dei formati ARN mostrati nella tabella seguente.

Il valore `partition` nell'ARN si riferisce a un gruppo di Regioni AWS. Ogni Account AWS è limitato a una partizione. Di seguito sono riportate le partizioni supportate:

- aws – Regioni AWS
- Regioni aws-us-gov - AWS GovCloud (US)

La tabella seguente mostra i formati ARN di S3 su Outposts.

Amazon S3 su ARN Outposts.	Formato ARN	Esempio
Bucket ARN	<code>arn:<i>partition</i> :s3-outposts: <i>region</i>: <i>account_id</i> :outpost / <i>outpost_id</i> / bucket/<i>bucket_name</i></code>	<code>arn:aws:s3-outpost:us-west-2:123456789012:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1</code>
ARN del punto di accesso	<code>arn:<i>partition</i> :s3-outposts: <i>region</i>: <i>account_id</i> :outpost / <i>outpost_id</i> /accesspoint/ <i>accesspoint_name</i></code>	<code>arn:aws:s3-outpost:us-west-2:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name</code>
Oggetto ARN	<code>arn:<i>partition</i> :s3-outposts: <i>region</i>: <i>account_id</i> :outpost / <i>outpost_id</i> / bucket/<i>bucket_name</i> / object/<i>object_key</i></code>	<code>arn:aws:s3-outpost:us-west-2:123456789012:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1/object/myobject</code>
ARN dell'oggetto punto di accesso S3 su Outpost (utilizzato nelle policy)	<code>arn:<i>partition</i> :s3-outposts: <i>region</i>: <i>account_id</i> :outpost / <i>outpost_id</i> /accesspoint/ <i>accesspoint_name</i> / object/<i>object_key</i></code>	<code>arn:aws:s3-outpost:us-west-2:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name/object/myobject</code>

Amazon S3 su ARN Outposts.	Formato ARN	Esempio
ARN di S3 su Outposts	<code>arn:<i>partition</i> :s3- outposts: <i>region</i>: <i>account_id</i> :outpost / <i>outpost_id</i></code>	<code>arn:aws:s3-outpo sts: us-west-2 :123456789012 : outpost/ op-01ac5d 28a6a232904</code>

Esempi di policy per S3 su Outposts

Example : policy del bucket S3 su Outposts con un principale Account AWS

La seguente policy del bucket utilizza un principale Account AWS per concedere l'accesso a un bucket S3 su Outposts. Per utilizzare questa policy del bucket, sostituisci *user input placeholders* con le tue informazioni.

Example : policy del bucket S3 su Outposts policy con principale e chiave di condizione con carattere jolly (*) per limitare l'accesso a un intervallo di indirizzi IP specifico.

La seguente policy del bucket utilizza un principale con carattere jolly (*) con la condizione `aws:SourceIp` per limitare l'accesso a un intervallo di indirizzi IP specifico. Per utilizzare questa policy del bucket, sostituisci *user input placeholders* con le tue informazioni.

Autorizzazioni per endpoint S3 su Outposts

S3 su Outposts richiede proprie autorizzazioni in IAM per gestire le operazioni degli endpoint S3 su Outposts.

Note

- Per gli endpoint che utilizzano il tipo di accesso del pool di indirizzi IP (pool CoIP) di proprietà del cliente, è inoltre necessario disporre delle autorizzazioni per lavorare con gli indirizzi IP del pool CoIP, come descritto nella tabella seguente.
- Per gli account condivisi che accedono a S3 su Outposts tramite AWS Resource Access Manager, gli utenti in questi account condivisi non possono creare i propri endpoint in una sottorete condivisa. Se un utente in un account condiviso desidera gestire i propri

endpoint, l'account condiviso deve creare una propria sottorete nell'Outpost. Per ulteriori informazioni, consulta [the section called “Condivisione di S3 su Outposts”](#).

La tabella seguente mostra le autorizzazioni IAM correlate agli endpoint S3 su Outposts.

Azione	Autorizzazioni IAM
CreateEndpoint	<code>s3-outposts:CreateEndpoint</code> <code>ec2:CreateNetworkInterface</code> <code>ec2:DescribeNetworkInterfaces</code> <code>ec2:DescribeVpcs</code> <code>ec2:DescribeSecurityGroups</code> <code>ec2:DescribeSubnets</code> <code>ec2:CreateTags</code> <code>iam:CreateServiceLinkedRole</code> Per gli endpoint che utilizzano il tipo di accesso del pool di indirizzi IP di proprietà del cliente on-premise (pool CoIP), sono necessarie le seguenti autorizzazioni aggiuntive: <code>s3-outposts:CreateEndpoint</code> <code>ec2:DescribeCoipPools</code> <code>ec2:GetCoipPoolUsage</code> <code>ec2:AllocateAddress</code> <code>ec2:AssociateAddress</code> <code>ec2:DescribeAddresses</code>

Azione	Autorizzazioni IAM
	ec2:DescribeLocalGatewayRouteTableVpcAssociations
DeleteEndpoint	<p>s3-outposts:DeleteEndpoint</p> <p>ec2:DeleteNetworkInterface</p> <p>ec2:DescribeNetworkInterfaces</p> <p>Per gli endpoint che utilizzano il tipo di accesso del pool di indirizzi IP di proprietà del cliente on-premise (pool ColIP), sono necessarie le seguenti autorizzazioni aggiuntive:</p> <p>s3-outposts:DeleteEndpoint</p> <p>ec2:DisassociateAddress</p> <p>ec2:DescribeAddresses</p> <p>ec2:ReleaseAddress</p>
ListEndpoints	s3-outposts>ListEndpoints

 Note

Puoi utilizzare i tag delle risorse in una policy IAM per gestire le autorizzazioni.

Ruoli collegati ai servizi per S3 su Outposts

S3 su Outposts utilizza ruoli IAM collegati ai servizi per creare alcune risorse di rete per tuo conto.

Per ulteriori informazioni, consulta [Utilizzo dei ruoli collegati ai servizi per Amazon S3 su Outposts](#).

Crittografia dei dati in S3 su Outposts

Per default, tutti i dati memorizzati in Amazon S3 su Outposts vengono crittografati utilizzando la crittografia lato server con chiavi di crittografia gestite di Amazon S3 (SSE-S3). Per ulteriori informazioni, consulta [Uso della crittografia lato server con chiavi gestite da Amazon S3 \(SSE-S3\)](#) nella Guida per l'utente di Amazon S3.

È possibile specificare la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C). Per utilizzare SSE-C, specifica una chiave di crittografia come parte delle richieste API sull'oggetto. La crittografia lato server viene applicata solo ai dati dell'oggetto, non dei metadati dell'oggetto. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi fornite dal cliente](#) nella Guida per l'utente di Amazon S3.

 Note

Amazon S3 su Outposts non supporta la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS).

AWS PrivateLink per S3 su Outposts

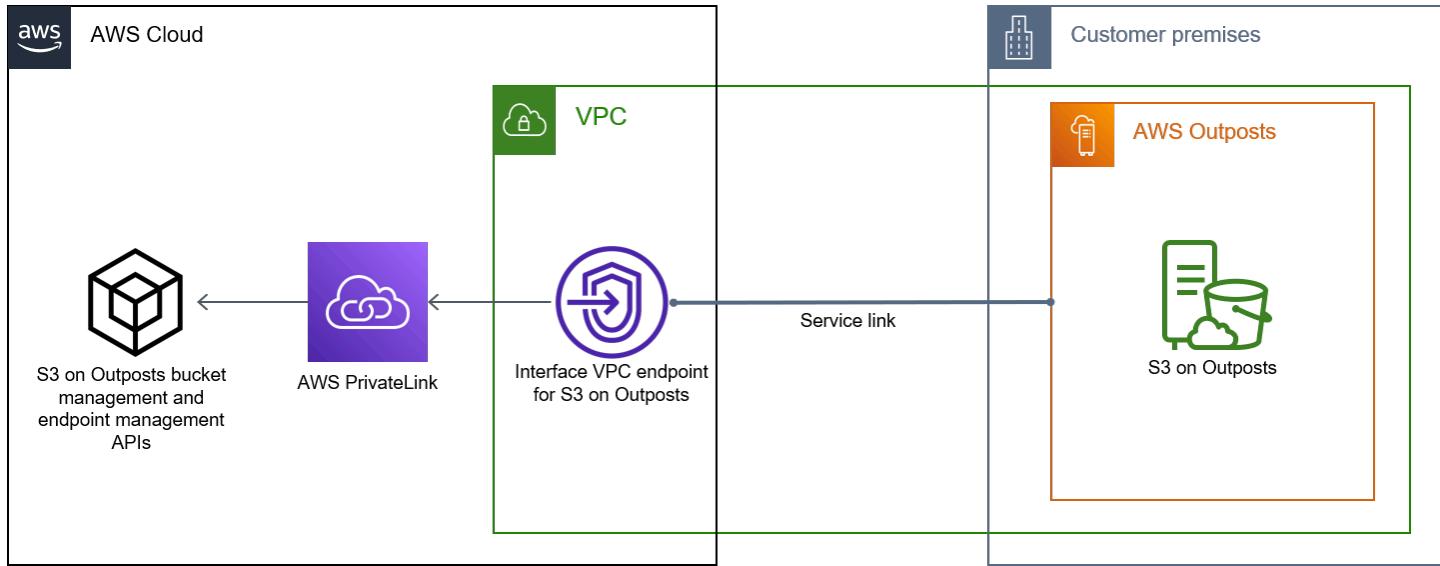
S3 su Outposts supporta AWS PrivateLink, che fornisce l'accesso di gestione diretto allo storage S3 su Outposts tramite un endpoint privato all'interno della rete privata virtuale. Ciò consente di semplificare l'architettura di rete interna ed eseguire operazioni di gestione sullo storage di oggetti Outposts utilizzando indirizzi IP privati nel cloud privato virtuale (VPC). L'uso di AWS PrivateLink elimina la necessità di utilizzare indirizzi IP pubblici o server proxy.

Con AWS PrivateLink per Amazon S3 su Outposts, puoi effettuare il provisioning degli endpoint VPC dell'interfaccia nel cloud privato virtuale (VPC) per accedere alle API di [gestione dei bucket](#) e di [gestione degli endpoint](#) di S3 su Outposts. Gli endpoint VPC dell'interfaccia sono accessibili alle applicazioni distribuite nel VPC o on-premise sulla rete privata virtuale (VPN) o AWS Direct Connect. Puoi accedere alle API di gestione bucket e di gestione degli endpoint tramite AWS PrivateLink. AWS PrivateLink non supporta le operazioni API di [trasferimento dati](#), come GET, PUT e API simili. Queste operazioni vengono già trasferite privatamente tramite la configurazione dell'endpoint e del punto di accesso S3 su Outposts. Per ulteriori informazioni, consulta [Reti per S3 su Outposts](#).

Gli endpoint di interfaccia sono rappresentati da una o più interfacce di rete elastiche (ENI) a cui vengono assegnati indirizzi IP privati dalle sottoreti nel VPC. Le richieste effettuate agli endpoint

dell'interfaccia per S3 su Outposts vengono instradate automaticamente alle API di gestione dei bucket e degli endpoint S3 su Outposts sulla rete AWS. È inoltre possibile accedere agli endpoint di interfaccia nel VPC da applicazioni locali tramite AWS Direct Connect o AWS Virtual Private Network (Site-to-Site VPN). Per ulteriori informazioni su come connettere il VPC alla rete On-Premise, consulta la [Guida per l'utente di Direct Connect](#) e la [Guida per l'utente di AWS Site-to-Site VPN](#).

Gli endpoint di interfaccia instradano le richieste per le API di gestione dei bucket e degli endpoint di S3 su Outposts sulla rete AWS e tramite AWS PrivateLink, come illustrato nello schema seguente.



Per informazioni sulla creazione di endpoint di interfaccia, consulta [Endpoint VPC di interfaccia \(AWS PrivateLink\)](#) nella Guida di AWS PrivateLink.

Argomenti

- [Restrizioni e limitazioni](#)
- [Accesso a endpoint dell'interfaccia S3 su Outposts](#)
- [Aggiornamento di una configurazione DNS locale](#)
- [Creazione di un endpoint VPC per S3 su Outposts](#)
- [Creazione di policy di bucket e policy di endpoint VPC per S3 su Outposts](#)

Restrizioni e limitazioni

Quando si accede alle API di gestione dei bucket e degli endpoint di S3 su Outposts tramite AWS PrivateLink, si applicano limitazioni VPC. Per ulteriori informazioni, consulta [Proprietà e limitazioni degli endpoint di interfaccia](#) e [Quote di AWS PrivateLink](#) nella Guida di AWS PrivateLink.

Inoltre, AWS PrivateLink non supporta quanto segue:

- [Endpoint FIPS \(Federal Information Processing Standard\)](#)
- [API di trasferimento dati S3 su Outposts](#), ad esempio, operazioni GET, PUT e API di oggetti simili.
- DNS privato

Accesso a endpoint dell'interfaccia S3 su Outposts

Per accedere alle API di gestione dei bucket e di gestione degli endpoint di S3 su Outposts utilizzando AWS PrivateLink, è necessario aggiornare le applicazioni in modo da utilizzare nomi DNS specifici degli endpoint. Quando crei un endpoint di interfaccia, AWS PrivateLink genera due tipi di nomi S3 su Outpost specifici dell'endpoint: regionale e zonale.

- I nomi DNS regionali includono un ID endpoint VPC univoco, un identificatore di servizio, Regione AWS e `vpce.amazonaws.com`, ad esempio, `vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com`.
- Nomi DNS zonali: includono un ID endpoint VPC univoco, la zona di disponibilità, un identificatore di servizio, Regione AWS e `vpce.amazonaws.com`, ad esempio, `vpce-1a2b3c4d-5e6f-us-east-1a.s3-outposts.us-east-1.vpce.amazonaws.com`. Puoi utilizzare questa opzione se l'architettura isola le zone di disponibilità. Ad esempio, puoi utilizzare i nomi DNS zonali per il contenimento degli errori o per ridurre i costi di trasferimento dei dati a livello regionale.

Important

Gli endpoint dell'interfaccia S3 su Outposts vengono risolti dal dominio DNS pubblico. S3 su Outposts non supporta il DNS privato. Usa il parametro `--endpoint-url` per tutte le API di gestione dei bucket e degli endpoint.

AWS CLI Esempi di

Utilizzo dei parametri `--region` e `--endpoint-url` per accedere alle API di gestione dei bucket e degli endpoint tramite gli endpoint dell'interfaccia S3 su Outposts.

Example : utilizzo dell'URL dell'endpoint per elencare i bucket con l'API di controllo S3

Nell'esempio seguente, sostituisci la Regione ***us-east-1***, l'URL endpoint VPC ***vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com*** e l'ID account ***111122223333*** con le informazioni appropriate.

```
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
```

AWSEsempi di SDK

Aggiorna gli SDK alla versione più recente e configura i client per utilizzare un URL endpoint per accedere all'API di controllo S3 per gli endpoint di interfaccia S3 su Outposts.

SDK for Python (Boto3)

Example : utilizzo di un URL endpoint per accedere all'API di controllo S3

Nell'esempio seguente, sostituisci la Regione ***us-east-1*** e l'URL endpoint VPC ***vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com*** con le informazioni appropriate.

```
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'  
)
```

Per ulteriori informazioni, consulta [AWS PrivateLink per Amazon S3](#) nella Guida per sviluppatori di Boto3.

SDK for Java 2.x

Example : utilizzo di un URL endpoint per accedere all'API di controllo S3

Nell'esempio seguente, sostituire l'URL endpoint VPC ***vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com*** e la Regione ***Region.US_EAST_1*** con le informazioni appropriate.

```
// 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()
```

Per ulteriori informazioni, consulta [S3ControlClient](#) nella documentazione di riferimento dell'API AWS SDK per Java.

Aggiornamento di una configurazione DNS locale

Quando si utilizzano nomi DNS specifici degli endpoint per accedere agli endpoint di interfaccia per le API di gestione degli endpoint e dei bucket S3 su Outposts, non è necessario aggiornare il resolver DNS locale. Puoi risolvere il nome DNS specifico dell'endpoint con l'indirizzo IP privato dell'endpoint di interfaccia dal dominio DNS di S3 su Outposts pubblico.

Creazione di un endpoint VPC per S3 su Outposts

Per creare un endpoint di interfaccia VPC per S3 su Outposts, vedere [Creare un endpoint VPC](#) nella Guida AWS PrivateLink.

Creazione di policy di bucket e policy di endpoint VPC per S3 su Outposts

Puoi allegare una policy di endpoint all'endpoint VPC che controlla l'accesso a S3 su Outposts.

Puoi utilizzare la condizione `aws:sourceVpce` nelle policy del bucket S3 su Outposts per limitare l'accesso a bucket specifici da un endpoint VPC specifico. Con le policy degli endpoint VPC, è possibile controllare l'accesso alle API di gestione dei bucket di S3 su Outposts e alle API di gestione degli endpoint. Con le policy dei bucket, è possibile controllare l'accesso alle API di gestione dei bucket S3 su Outposts. Tuttavia, non è possibile gestire l'accesso alle azioni oggetto per S3 su Outposts utilizzando `aws:sourceVpce`.

Le policy di accesso per S3 su Outposts specificano le seguenti informazioni:

- Il principal AWS Identity and Access Management (IAM) per il quale le operazioni sono consentite o rifiutate.
- Le operazioni di controllo S3 consentite o rifiutate.
- Le risorse S3 su Outposts su cui le operazioni sono consentite o rifiutate.

Negli esempi seguenti vengono illustrate le policy che limitano l'accesso a un bucket o a un endpoint. Per maggiori informazioni sulla connettività VPC, consulta [Opzioni di connettività da rete a VPC](#) nel whitepaper AWS [Opzioni di connettività di Amazon Virtual Private Cloud](#).

Important

- Quando applichi le policy di esempio per gli endpoint VPC descritte in questa sezione, potresti bloccare involontariamente l'accesso al bucket. Le autorizzazioni del bucket che limitano l'accesso del bucket a connessioni originate dall'endpoint VPC possono bloccare tutte le connessioni al bucket. Per informazioni su come risolvere questo problema, consulta [La policy del bucket ha l'ID del VPC o dell'endpoint VPC sbagliato. Come posso correggere la policy in modo da poter accedere al bucket?](#) nel Knowledge Center di Supporto.
- Prima di utilizzare le policy di esempio seguenti, sostituire l'ID endpoint VPC con un valore appropriato per il caso d'uso. In caso contrario, non sarà possibile accedere al bucket.
- Se la policy consente l'accesso a un bucket S3 su Outposts da uno specifico endpoint VPC, disabilita l'accesso alla console per quel bucket in quanto le richieste della console non provengono dall'endpoint VPC specificato.

Argomenti

- [Esempio: limitazione dell'accesso a un bucket specifico da un endpoint VPC](#)
- [Esempio: negazione dell'accesso da un endpoint VPC specifico in una policy del bucket S3 su Outposts](#)

Esempio: limitazione dell'accesso a un bucket specifico da un endpoint VPC

Puoi creare una policy di endpoint che limita l'accesso solo a bucket S3 su Outposts specifici. La seguente policy limita l'accesso per l'azione GetBucketPolicy solo a *example-outpost-bucket*. Per usare questa policy, sostituire i valori di esempio con i propri.

JSON

```
{  
  "Version": "2012-10-17",  
  "Id": "Policy1415115909151",  
  "Statement": [  
    {"Sid": "AllowGetBucketPolicy", "Effect": "Allow", "Action": "s3:GetBucketPolicy", "Resource": "arn:aws:s3:::example-outpost-bucket"}  
  ]}
```

```

"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"
  }
]
}

```

Esempio: negazione dell'accesso da un endpoint VPC specifico in una policy del bucket S3 su Outposts

La seguente policy del bucket S3 su Outposts nega l'accesso a GetBucketPolicy nel bucket *example-outpost-bucket* attraverso l'endpoint VPC *vpce-1a2b3c4d*.

La condizione `aws:sourceVpce` viene utilizzata per specificare l'endpoint e non richiede un Amazon Resource Name (ARN) per la risorsa dell'endpoint VPC, ma solo l'ID dell'endpoint. Per usare questa policy, sostituire i valori di esempio con i propri.

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"
    }
}
]
}

```

Chiavi di policy specifiche per l'autenticazione con AWS Signature Version 4 (SigV4)

La tabella seguente mostra le chiavi di condizione relative a AWS Signature Version 4 (SigV4) che puoi utilizzare con Amazon S3 su Outposts. In una policy del bucket, puoi aggiungere queste condizioni per applicare un comportamento specifico quando le richieste vengono autenticate tramite Signature Version 4. Per esempi di policy, consulta [Esempi di policy del bucket che utilizzano chiavi di condizione relative a Signature Version 4](#). Per ulteriori informazioni sull'autenticazione delle richieste tramite Signature Version 4, consulta [Autenticazione delle richieste \(AWS Signature Version 4\)](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Chiavi applicabili	Descrizione
s3-outpos ts:authType	<p>S3 su Outposts supporta diversi metodi di autenticazione. Per limitare le richieste in arrivo all'utilizzo di un metodo di autenticazione specifico, puoi utilizzare questa chiave di condizione opzionale. Ad esempio, puoi utilizzare questa chiave di condizione per consentire solo l'intestazione <code>Authorization</code> HTTP da utilizzare nell'autenticazione della richiesta.</p> <p>Valori validi:</p> <ul style="list-style-type: none"> REST-HEADER REST-QUERY-STRING
s3-outpos ts:signature eAge	Il periodo di tempo, espresso in millisecondi, di validità di una firma in una richiesta autenticata.
	Questa condizione è valida solo per gli URL prefirmati.

Chiavi applicabili	Descrizione
	<p>In Signature Version 4, la chiave di firma è valida per un massimo di sette giorni. Pertanto, anche le firme sono valide per un massimo di sette giorni. Per ulteriori informazioni, consulta Introduzione alla firma delle richieste nella Documentazione di riferimento delle API di Amazon Simple Storage Service. Puoi utilizzare questa condizione per limitare ulteriormente la durata della firma.</p> <p>Valore di esempio: 600000</p>
s3-outposts:x-amz-content-sha256	<p>Questa chiave di condizione può essere utilizzata per non consentire contenuti non firmati nel bucket.</p> <p>Quando utilizzi Signature Version 4, per le richieste che utilizzano l'intestazione <code>Authorization</code>, aggiungi l'intestazione <code>x-amz-content-sha256</code> nel calcolo della firma e quindi imposti il suo valore sul payload hash.</p> <p>Questa chiave di condizione può essere utilizzata nella policy del bucket per negare qualsiasi caricamento in cui i payload non sono firmati. Ad esempio:</p> <ul style="list-style-type: none"> • Nega i caricamenti che utilizzano l'intestazione <code>Authorization</code> per autenticare le richieste ma non firmare il payload. Per ulteriori informazioni, consulta Trasferimento del carico utile in un unico blocco nella Documentazione di riferimento delle API di Amazon Simple Storage Service. • Nega i caricamenti che utilizzano gli URL prefirmati. Gli URL prefirmati hanno sempre un <code>UNSIGNED_PAYLOAD</code>. Per ulteriori informazioni, consulta la sezione Autenticazione delle richieste e Metodi di autenticazione nella Documentazione di riferimento delle API di Amazon Simple Storage Service. <p>Valore valido: <code>UNSIGNED-PAYLOAD</code></p>

Esempi di policy del bucket che utilizzano chiavi di condizione relative a Signature Version 4

Per utilizzare i seguenti esempi, sostituisci *user input placeholders* con le tue informazioni.

Example : **s3-outposts:signatureAge**

La seguente policy del bucket nega qualsiasi richiesta di URL prefirmato S3 su Outposts sugli oggetti in example-outpost-bucket se la firma è più vecchia di 10 minuti.

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": "44445556666"},  
            "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**

La seguente policy del bucket consente solo le richieste che utilizzano l'intestazione Authorization per l'autenticazione della richiesta. Qualsiasi richiesta di URL prefirmato verrà negata poiché gli URL prefirmati utilizzano parametri di query per fornire informazioni di richiesta e autenticazione. Per ulteriori informazioni, consulta [Metodi di autenticazione](#) nella Documentazione di riferimento delle API di 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**

La seguente policy del bucket nega qualsiasi caricamento con payload non firmati, ad esempio quelli che utilizzano URL prefirmati. Per ulteriori informazioni, consulta la sezione [Autenticazione delle richieste](#) e [Metodi di autenticazione](#) nella Documentazione di riferimento delle API di 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"  
            }  
        }  
    }  
}
```

Policy gestite da AWS per Amazon S3 su Outposts

Una policy gestita da AWS è una policy autonoma creata e amministrata da AWS. Le policy gestite da AWS sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tenere presente che le policy gestite da AWS potrebbero non concedere autorizzazioni con privilegi minimi per i casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWS aggiorni una policy gestita da AWS quando viene lanciato un nuovo Servizio AWS o nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

Policy gestita da AWS: AWSS3OnOutpostsServiceRolePolicy

Aiuta a gestire le risorse di rete per l'utente come parte del ruolo collegato al servizio AWSServiceRoleForS3OnOutposts.

Per visualizzare le autorizzazioni per questa policy, consulta [AWSS3OnOutpostsServiceRolePolicy](#).

Aggiornamenti di Amazon S3 su Outposts sulle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per Amazon S3 su Outposts da quando questo servizio ha iniziato a tenere traccia delle modifiche.

Modifica	Descrizione	Data
S3 su Outposts ha aggiunto AWSS3OnOutpostsServiceRolePolicy	S3 su Outposts ha aggiunto AWSS3OnOutpostsServiceRolePolicy come parte del ruolo collegato al servizio AWSServiceRoleForS3OnOutposts per aiutare a gestire le risorse di rete per conto dell'utente.	3 ottobre 2023
S3 su Outposts ha iniziato a tenere traccia delle modifiche	S3 su Outposts ha iniziato a tenere traccia delle modifiche per le sue policy gestite da AWS.	3 ottobre 2023

Utilizzo dei ruoli collegati ai servizi per Amazon S3 su Outposts

Amazon S3 su Outposts utilizza i [ruoli collegati ai servizi](#) AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a S3 su Outposts. I ruoli collegati ai servizi sono predefiniti da S3 su Outposts e includono tutte le autorizzazioni necessarie al servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di S3 su Outposts perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. S3 su Outposts definisce le autorizzazioni dei relativi ruoli collegati ai servizi e, salvo diversamente definito, solo S3 su Outposts potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di S3 su Outposts perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per S3 su Outposts

S3 su Outposts utilizza il ruolo collegato ai servizi denominato AWSServiceRoleForS3OnOutposts per aiutarti a gestire le risorse di rete.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForS3OnOutposts considera attendibili i seguenti servizi:

- `s3-outposts.amazonaws.com`

La policy delle autorizzazioni del ruolo denominata AWSS3OnOutpostsServiceRolePolicy consente a S3 su Outposts di eseguire le seguenti operazioni sulle risorse specificate:

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"
```

```
    }  
]  
}
```

Per consentire a un'entità IAM (come un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per S3 su Outposts

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un endpoint S3 su Outposts nella Console di gestione AWS, nella AWS CLI o nell'API AWS, S3 su Outposts crea automaticamente il ruolo collegato ai servizi.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un endpoint S3 su Outposts, esso crea automaticamente il ruolo collegato ai servizi.

Puoi utilizzare la console IAM anche per creare un ruolo collegato ai servizi con il caso d'uso S3 su Outposts. In AWS CLI o in AWS API, crea un ruolo collegato al servizio con il nome di servizio `s3-outposts.amazonaws.com`. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per S3 su Outposts

S3 su Outposts non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForS3OnOutposts`. Questo include il nome del ruolo perché varie entità possano farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per S3 su Outposts

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Note

Se il servizio S3 su Outposts utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non riesca. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse S3 su Outposts utilizzate dal ruolo `AWSServiceRoleForS3OnOutposts`

1. [Elimina gli endpoint S3 su Outposts](#) nel tuo Account AWS in tutte le Regioni AWS.
2. Eliminazione del ruolo collegato ai servizi utilizzando IAM.

Utilizzare la console IAM, AWS CLI, la AWS o l'API per eliminare i ruoli collegati ai servizi `AWSServiceRoleForS3OnOutposts`. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di S3 su Outposts

S3 su Outposts supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni AWS in cui il servizio è disponibile. Per ulteriori informazioni, consulta [S3 on Outposts Regions and endpoints](#).

Gestione dello storage S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta . [Che cos'è Amazon S3 su Outposts?](#)

Per ulteriori informazioni su come gestire e condividere la capacità di archiviazione di Amazon S3 su Outposts, consulta i seguenti argomenti.

Argomenti

- [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#)
- [Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts](#)
- [Replica degli oggetti per S3 su Outposts](#)
- [Condivisione di S3 on Outposts tramite AWS RAM](#)
- [Altri Servizi AWS che utilizzano S3 su Outposts](#)

Gestione del controllo delle versioni S3 per il bucket S3 su Outposts

Se abilitato, il controllo delle versioni S3 conserva più copie distinte di un oggetto nello stesso bucket. Puoi utilizzare il controllo delle versioni S3 per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nei bucket Outposts. Il controllo delle versioni S3 ti consente di eseguire il ripristino a seguito di errori dell'applicazione e operazioni non intenzionali degli utenti.

I bucket Amazon S3 su Outposts hanno tre stati del controllo delle versioni:

- **Unversioned (Senza versione):** se non hai mai abilitato o sospeso il controllo delle versioni S3 per il tuo bucket, non viene eseguito alcun controllo delle versioni e non viene restituito lo stato

del controllo delle versioni S3. Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#).

- Enabled (Abilitato): il controllo delle versioni S3 è abilitato per gli oggetti nel bucket. A tutti gli oggetti aggiunti al bucket viene assegnato un ID versione univoco. Gli oggetti già esistenti nel bucket al momento dell'attivazione del controllo delle versioni hanno un ID versione null. Se modifichi questi o altri oggetti con altre operazioni, come [PutObject](#), i nuovi oggetti ottengono un ID versione univoco.
- Suspended (Sospeso): il controllo delle versioni S3 è sospeso per gli oggetti nel bucket. A tutti gli oggetti aggiunti al bucket dopo la sospensione del controllo delle versioni verrà assegnato l'ID versione null. Per ulteriori informazioni, consulta [Aggiunta di oggetti a bucket con funzionalità controllo delle versioni sospeso](#) nella Guida per l'utente di Amazon S3.

Dopo aver abilitato il controllo delle versioni S3 per un bucket S3 su Outposts, non è possibile ripristinare lo stato senza versione del bucket. Tuttavia, puoi sospendere il controllo delle versioni. Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#).

Per ogni oggetto nel bucket esistono una versione corrente e nessuna o più versioni non correnti. Per ridurre i costi di archiviazione, puoi configurare le regole del ciclo di vita del bucket S3 in modo che le versioni non correnti scadano dopo un periodo di tempo specificato. Per ulteriori informazioni, consulta [Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts](#).

Negli esempi seguenti viene illustrato come abilitare o sospendere il controllo delle versioni per un bucket S3 su Outposts utilizzando la Console di gestione AWS e AWS Command Line Interface (AWS CLI). Per creare un bucket con il controllo delle versioni S3 abilitato, consulta [Creazione di un bucket S3 su Outposts](#).

Note

L'Account AWS che crea il bucket lo possiede ed è l'unico che può eseguire azioni su di esso. I bucket dispongono di proprietà di configurazione come Outpost, tag, crittografia di default e impostazioni del punto di accesso. Le impostazioni del punto di accesso includono il Virtual Private Cloud (VPC), la policy del punto di accesso per l'accesso agli oggetti nel bucket e altri metadati. Per ulteriori informazioni, consulta [Specifiche di S3 su Outposts](#).

Utilizzo della console S3

Modifica delle impostazioni del controllo delle versioni S3 per il bucket

1. Accedere a Console di gestione AWS e aprire la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Scegli il bucket Outposts per cui desideri abilitare il controllo delle versioni S3.
4. Scegliere la scheda Properties (Proprietà).
5. In Bucket Versioning (Funzione Controllo delle versioni del bucket) scegliere Edit (Modifica).
6. Modifica le impostazioni del controllo delle versioni S3 per il bucket scegliendo una delle seguenti opzioni:
 - Per sospendere il controllo delle versioni S3 e interrompere la creazione di nuove versioni per gli oggetti, scegli Suspend (Sospendi).
 - Per abilitare il controllo delle versioni S3 e salvare più copie distinte di ciascun oggetto, scegli Enable (Abilita).
7. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Per abilitare o sospendere il controllo delle versioni S3 per il bucket utilizzando AWS CLI, usa il comando `put-bucket-versioning` come mostrato negli esempi seguenti. Per usare questi esempi, sostituisci ciascun *user input placeholder* con le tue informazioni.

Per ulteriori informazioni, vedi [put-bucket-versioning](#) in AWS CLI Reference.

Example - Abilitazione del controllo delle versioni 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 - Sospensione del controllo delle versioni 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
```

Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts

È possibile utilizzare il ciclo di vita S3 per ottimizzare la capacità di archiviazione per Amazon S3 su Outposts. È possibile creare regole del ciclo di vita per far scadere gli oggetti man mano che invecchiano o vengono sostituiti da versioni più recenti. Puoi creare, abilitare, disabilitare o eliminare una regola del ciclo di vita.

Per ulteriori informazioni sul ciclo di vita S3, consulta [Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts](#).

Note

L'Account AWS che crea il bucket lo possiede ed è l'unico in grado di creare, abilitare, disabilitare o eliminare una regola del ciclo di vita.

Per creare e gestire la configurazione del ciclo di vita per un bucket S3 su Outposts, consulta i seguenti argomenti.

Argomenti

- [Creazione e gestione di una regola del ciclo di vita utilizzando Console di gestione AWS](#)
- [Creazione e gestione di una configurazione del ciclo di vita utilizzando AWS CLI e SDK per Java](#)

Creazione e gestione di una regola del ciclo di vita utilizzando Console di gestione AWS

È possibile utilizzare il ciclo di vita S3 per ottimizzare la capacità di archiviazione per Amazon S3 su Outposts. È possibile creare regole del ciclo di vita per far scadere gli oggetti man mano che invecchiano o vengono sostituiti da versioni più recenti. Puoi creare, abilitare, disabilitare o eliminare una regola del ciclo di vita.

Per ulteriori informazioni sul ciclo di vita S3, consulta [Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts](#).

Note

L'Account AWS che crea il bucket lo possiede ed è l'unico in grado di creare, abilitare, disabilitare o eliminare una regola del ciclo di vita.

Per creare e gestire una regola del ciclo di vita per S3 su Outposts utilizzando la Console di gestione AWS, consulta i seguenti argomenti.

Argomenti

- [Creazione di una regola del ciclo di vita](#)
- [Abilitazione di una regola del ciclo di vita](#)
- [Modifica di una regola del ciclo di vita](#)
- [Eliminazione di una regola del ciclo di vita](#)

Creazione di una regola del ciclo di vita

1. Accedi alla Console di gestione AWS e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts per il quale desideri creare una regola del ciclo di vita.
4. Seleziona la scheda Gestione, quindi Crea regola ciclo di vita.
5. Inserisci un valore per Lifecycle rule name (Nome della regola del ciclo di vita).
6. In Rule scope (Ambito della regola) scegli una delle opzioni seguenti:
 - Per limitare l'ambito di questa regola a filtri specifici, scegli Limit the scope of this rule using one or more filters (Limita l'ambito di questa regola utilizzando uno o più filtri). Quindi, aggiungi un filtro prefisso, i tag o la dimensione dell'oggetto.
 - Per applicare questa regola del ciclo di vita a tutti gli oggetti del bucket, scegli Apply to all objects in the bucket (Applica a tutti gli oggetti nel bucket).
7. In Lifecycle rule actions (Operazioni regola del ciclo di vita), scegli una delle seguenti opzioni:
 - Expire current versions of objects (Scadenza versioni correnti degli oggetti): per i bucket con il controllo delle versioni abilitato, S3 su Outposts aggiunge un contrassegno di eliminazione e

mantiene gli oggetti come versioni non correnti. Per i bucket che non utilizzano il controllo delle versioni S3, S3 su Outposts elimina definitivamente gli oggetti.

- Permanently delete noncurrent versions of objects (Elimina definitivamente le versioni non correnti degli oggetti): S3 su Outposts elimina definitivamente le versioni non correnti degli oggetti.
- Delete expired object delete markers or incomplete multipart uploads (Elimina contrassegni di eliminazione oggetti scaduti o caricamenti in più parti incompleti): S3 su Outposts elimina definitivamente i contrassegni di eliminazione degli oggetti scaduti o i caricamenti in più parti incompleti.

Se limiti l'ambito della regola del ciclo di vita utilizzando i tag degli oggetti, non puoi scegliere Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti scaduti). Inoltre, non puoi scegliere Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti) se scegli Expire current object versions (Scadenza versioni correnti degli oggetti).

 Note

I filtri basati sulle dimensioni non possono essere utilizzati con i contrassegni di eliminazione e i caricamenti in più parti incompleti.

8. Se hai scelto Expire current versions of objects (Scadenza versioni correnti degli oggetti) o Permanently delete noncurrent versions of objects (Elimina definitivamente le versioni non correnti degli oggetti), configura il trigger della regola in base a una data specifica o all'età dell'oggetto.
9. Se hai scelto Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti scaduti), per confermare che desideri eseguire l'operazione di eliminazione, seleziona Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti scaduti).
10. In Timeline Summary (Riepilogo della cronologia), rivedi la regola del ciclo di vita e scegli Create rule (Crea regola).

Abilitazione di una regola del ciclo di vita

Per abilitare o disabilitare una regola del ciclo di vita del bucket

1. Apri la console Amazon S3 su <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts per cui desideri abilitare o disabilitare una regola del ciclo di vita.
4. Seleziona la scheda Management (Gestione), quindi in Lifecycle rule (Regola del ciclo di vita) scegli la regola del ciclo di vita che desideri abilitare o disabilitare.
5. Per Azione, scegli Abilita o disabilita regola.

Modifica di una regola del ciclo di vita

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts per il quale desideri modificare una regola del ciclo di vita.
4. Seleziona la scheda Gestione e scegli la regola del ciclo di vita che desideri modificare.
5. (Facoltativo) Aggiorna il valore in Lifecycle rule name (Nome della regola del ciclo di vita).
6. In Rule scope (Ambito della regola), modifica l'ambito secondo le necessità:
 - Per limitare l'ambito di questa regola a filtri specifici, scegli Limit the scope of this rule using one or more filters (Limita l'ambito di questa regola utilizzando uno o più filtri). Quindi, aggiungi un filtro prefisso, i tag o la dimensione dell'oggetto.
 - Per applicare questa regola del ciclo di vita a tutti gli oggetti del bucket, scegli Apply to all objects in the bucket (Applica a tutti gli oggetti nel bucket).
7. In Lifecycle rule actions (Operazioni regola del ciclo di vita), scegli una delle seguenti opzioni:
 - Expire current versions of objects (Scadenza versioni correnti degli oggetti): per i bucket con il controllo delle versioni abilitato, S3 su Outposts aggiunge un contrassegno di eliminazione e mantiene gli oggetti come versioni non correnti. Per i bucket che non utilizzano il controllo delle versioni S3, S3 su Outposts elimina definitivamente gli oggetti.
 - Permanently delete noncurrent versions of objects (Elimina definitivamente le versioni non correnti degli oggetti): S3 su Outposts elimina definitivamente le versioni non correnti degli oggetti.

- Delete expired object delete markers or incomplete multipart uploads (Elimina contrassegni di eliminazione oggetti scaduti o caricamenti in più parti incompleti): S3 su Outposts elimina definitivamente i contrassegni di eliminazione degli oggetti scaduti o i caricamenti in più parti incompleti.

Se limiti l'ambito della regola del ciclo di vita utilizzando i tag degli oggetti, non puoi scegliere Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti scaduti). Inoltre, non puoi scegliere Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti) se scegli Expire current object versions (Scadenza versioni correnti degli oggetti).

 Note

I filtri basati sulle dimensioni non possono essere utilizzati con i contrassegni di eliminazione e i caricamenti in più parti incompleti.

8. Se hai scelto Expire current versions of objects (Scadenza versioni correnti degli oggetti) o Permanently delete noncurrent versions of objects (Elimina definitivamente le versioni non correnti degli oggetti), configura il trigger della regola in base a una data specifica o all'età dell'oggetto.
9. Se hai scelto Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti scaduti), per confermare che desideri eseguire l'operazione di eliminazione, seleziona Delete expired object delete markers (Elimina i contrassegni di eliminazione degli oggetti scaduti).
10. Selezionare Salva.

Eliminazione di una regola del ciclo di vita

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il bucket Outposts per il quale desideri eliminare una regola del ciclo di vita.
4. Seleziona la scheda Management (Gestione), quindi in Lifecycle rule (Regola del ciclo di vita) scegli la regola del ciclo di vita che desideri eliminare.
5. Scegli Delete (Elimina).

Creazione e gestione di una configurazione del ciclo di vita utilizzando AWS CLI e SDK per Java

È possibile utilizzare il ciclo di vita S3 per ottimizzare la capacità di archiviazione per Amazon S3 su Outposts. È possibile creare regole del ciclo di vita per far scadere gli oggetti man mano che invecchiano o vengono sostituiti da versioni più recenti. Puoi creare, abilitare, disabilitare o eliminare una regola del ciclo di vita.

Per ulteriori informazioni sul ciclo di vita S3, consulta [Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts](#).

Note

L'Account AWS che crea il bucket lo possiede ed è l'unico in grado di creare, abilitare, disabilitare o eliminare una regola del ciclo di vita.

Per creare e gestire una configurazione del ciclo di vita per un bucket S3 su Outposts utilizzando AWS Command Line Interface (AWS CLI) e AWS SDK per Java, consulta i seguenti esempi.

Argomenti

- [PUT di una configurazione del ciclo di vita](#)
- [GET di una configurazione del ciclo di vita in un bucket S3 su Outposts](#)

PUT di una configurazione del ciclo di vita

AWS CLI

Nel seguente esempio della AWS CLI viene inserito una policy di configurazione del ciclo di vita in un bucket Outposts. Questa policy specifica che tutti gli oggetti con il prefisso contrassegnato (*myprefix*) e i tag scadono dopo 10 giorni. Per utilizzare questo comando, sostituisci *user input placeholder* con le tue informazioni.

1. Salva la policy di configurazione del ciclo di vita in un file JSON. In questo esempio, il file è denominato `lifecycle1.json`.

```
{  
  "Rules": [  
    {
```

```

{
    "ID": "id-1",
    "Filter": {
        "And": {
            "Prefix": "myprefix",
            "Tags": [
                {
                    "Value": "mytagvalue1",
                    "Key": "mytagkey1"
                },
                {
                    "Value": "mytagvalue2",
                    "Key": "mytagkey2"
                }
            ],
            "ObjectSizeGreaterThanOrEqual": 1000,
            "ObjectSizeLessThanOrEqual": 5000
        }
    },
    "Status": "Enabled",
    "Expiration": {
        "Days": 10
    }
}
]
}

```

2. Inviare il file JSON come parte del comando CLI `put-bucket-lifecycle-configuration`. Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [put-bucket-lifecycle-configuration](#) nella Guida di riferimento di 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

Nel seguente esempio di SDK for Java viene inserita una policy di configurazione del ciclo di vita in un bucket Outposts. La configurazione del ciclo di vita specifica che tutti gli oggetti con il prefisso contrassegnato (*myprefix*) e i tag scadono dopo 10 giorni. Per utilizzare

questo comando, sostituisci *user input placeholder* con le tue informazioni. Per ulteriori informazioni, consulta l'argomento relativo a [PutBucketLifecycleConfiguration](#) nella Documentazione di riferimento dell'API di 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());

}
```

GET di una configurazione del ciclo di vita in un bucket S3 su Outposts

AWS CLI

Nel seguente esempio della AWS CLI viene ottenuta una configurazione del ciclo di vita in un bucket Outposts. Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni. Per ulteriori informazioni su questo comando, consulta [get-bucket-lifecycle-configuration](#) nella Guida di riferimento di 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

Nel seguente esempio di SDK for Java viene ottenuta una configurazione del ciclo di vita per un bucket Outposts. Per ulteriori informazioni, consulta [GetBucketLifecycleConfiguration](#) nella Documentazione di riferimento delle API di 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());  
  
}
```

Replica degli oggetti per S3 su Outposts

Se la funzionalità Replica Amazon S3 è impostata su AWS Outposts, puoi configurare Amazon S3 su Outposts in modo che esegua automaticamente la replica degli oggetti S3 su outpost diversi o tra bucket nello stesso outpost. Puoi utilizzare Replica Amazon S3 su Outposts per gestire più replicate

dei tuoi dati nello stesso outpost o in outpost diversi oppure in account diversi, in modo conforme ai requisiti di residenza dei dati. Replica Amazon S3 su Outposts consente di potenziare i tuoi requisiti di conformità dell'archiviazione e la condivisione dei dati tra account. Se devi essere sicuro che le replica siano identiche ai dati di origine, puoi utilizzare Replica Amazon S3 su Outposts per creare repliche degli oggetti che mantengono tutti i metadati, ad esempio l'ora di creazione dell'oggetto originale, i tag e gli ID versione.

Replica Amazon S3 su Outposts fornisce anche metriche e notifiche dettagliate per monitorare lo stato della replica degli oggetti tra bucket. Puoi utilizzare Amazon CloudWatch per monitorare l'avanzamento della replica monitorando i byte in attesa di replica, le operazioni in attesa di replica e la latenza di replica tra i bucket di origine e destinazione. Per diagnosticare e correggere rapidamente i problemi di configurazione, puoi anche configurare Amazon EventBridge in modo da ricevere notifiche relative agli errori di replica degli oggetti. Per ulteriori informazioni, consulta [Gestione della replica](#).

Argomenti

- [Configurazione di replica](#)
- [Requisiti di Replica Amazon S3 su Outposts](#)
- [Elementi replicati](#)
- [Elementi non replicati](#)
- [Cosa non è supportato da Replica Amazon S3 su Outposts?](#)
- [Impostazione della replica](#)
- [Gestione della replica](#)

Configurazione di replica

S3 su Outposts archivia la configurazione della replica come file XML. Nel file XML della configurazione della replica è necessario specificare un ruolo AWS Identity and Access Management (IAM) e una o più regole.

```
<ReplicationConfiguration>
  <Role>IAM-role-ARN</Role>
  <Rule>
    ...
  </Rule>
  <Rule>
    ...
  </Rule>
```

```
</Rule>
...
</ReplicationConfiguration>
```

S3 su Outposts non può replicare oggetti senza la tua autorizzazione. Le autorizzazioni S3 su Outposts vengono concesse con il ruolo IAM specificato nella configurazione della replica. S3 su Outposts assume il ruolo IAM per replicare gli oggetti per tuo conto. È necessario concedere le autorizzazioni necessarie per il ruolo IAM prima di avviare la replica. Per ulteriori informazioni su queste autorizzazioni per S3 su Outposts, consulta [Creazione di un ruolo IAM](#).

Puoi aggiungere una regola a una configurazione di replica quando:

- Vuoi replicare tutti gli oggetti.
- Vuoi replicare un sottoinsieme di oggetti. Identifichi il sottoinsieme di oggetti aggiungendo un filtro alla regola. Nel filtro specifichi un prefisso di chiave o tag dell'oggetto o una combinazione di questi elementi, per identificare il sottoinsieme di oggetti a cui si applica la regola.

Per replicare più sottoinsiemi di oggetti, aggiungi diverse regole a una configurazione di replica. In ogni regola puoi specificare un filtro tramite cui selezionare un particolare sottoinsieme di oggetti. Puoi ad esempio scegliere di replicare gli oggetti con prefissi della chiave `tax/` o `document/`. Per fare ciò devi aggiungere due regole: una che specifica il filtro prefisso della chiave `tax/` e un'altra che specifica il prefisso della chiave `document/`.

Per ulteriori informazioni sulla configurazione e sulle regole per la replica in S3 su Outposts, consulta [ReplicationConfiguration](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Requisiti di Replica Amazon S3 su Outposts

La replica richiede quanto segue:

- L'intervallo CIDR Outpost di destinazione deve essere associato alla tabella della sottorete Outpost di origine. Per ulteriori informazioni, consulta [Prerequisiti per la creazione delle regole di replica](#).
- Sia per il bucket di origine che per quello di destinazione deve essere abilitata la funzione S3 di controllo delle versioni. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Gestione del controllo delle versioni S3 per il bucket S3 su Outposts](#).

- Amazon S3 su Outposts deve disporre dell'autorizzazione necessaria per replicare gli oggetti dal bucket di origine a quello di destinazione per tuo conto. Ciò significa che devi creare un ruolo di servizio da delegare GET e PUT le autorizzazioni a S3 su Outposts.
 1. Prima di creare il ruolo di servizio, è necessario disporre dell'autorizzazione GET sul bucket di origine e dell'autorizzazione PUT sul bucket di destinazione.
 2. Per creare il ruolo di servizio per delegare le autorizzazioni a S3 su Outposts, devi prima configurare le autorizzazioni per consentire a un'entità IAM (un utente o un ruolo) di eseguire le operazioni `iam:CreateRole` e `iam:PassRole`. Autorizza quindi l'entità IAM a creare il ruolo di servizio. Per fare in modo che S3 su Outposts assuma il ruolo di servizio per tuo conto e deleghi le autorizzazioni GET e PUT a S3 su Outposts, devi assegnare le necessarie policy di affidabilità e autorizzazione al ruolo. Per ulteriori informazioni su queste autorizzazioni per S3 su Outposts, consulta [Creazione di un ruolo IAM](#). Per ulteriori informazioni sulla creazione di un ruolo di servizio, consulta la sezione relativa alla [creazione di un ruolo di servizio](#).

Elementi replicati

Per impostazione predefinita, S3 su Outposts replica quanto segue:

- Oggetti creati dopo l'aggiunta di una configurazione di replica.
- Metadati dell'oggetto dagli oggetti di origine alle repliche. Per informazioni su come replicare i metadati dalle repliche agli oggetti di origine, consulta [Stato della replica se su Outposts è abilitata la sincronizzazione della modifica della replica Amazon S3](#).
- Eventuali tag degli oggetti.

Effetto delle operazioni di eliminazione sulla replica

Se si elimina un oggetto dal bucket di origine, per impostazione predefinita si verificano le seguenti azioni:

- Se effettui una richiesta `DELETE` senza specificare l'ID versione dell'oggetto, S3 su Outposts aggiunge un contrassegno di eliminazione. S3 su Outposts gestisce il contrassegno di eliminazione in questo modo:
 - S3 su Outposts non replica il contrassegno di eliminazione per impostazione predefinita.
 - Tuttavia, puoi aggiungere la replica del contrassegno di eliminazione a regole non basate su tag. Per ulteriori informazioni su come abilitare la replica dei contrassegni di eliminazione nella configurazione della replica, consulta [Utilizzo della console S3](#).

- Se in una richiesta DELETE specifichi l'ID versione di un oggetto da eliminare, S3 su Outposts elimina la versione dell'oggetto nel bucket di origine. Non viene tuttavia eseguita la replica dell'eliminazione nel bucket di destinazione. In altre parole, non elimina la stessa versione dell'oggetto dai bucket di destinazione. Questo comportamento permette di proteggere i dati da eliminazioni da parte di utenti malintenzionati.

Elementi non replicati

Per impostazione predefinita, S3 su Outposts non replica quanto segue:

- Gli oggetti nel bucket di origine che sono repliche create da un'altra regola di replica. Supponiamo, per esempio, di configurare una replica dove il bucket A è l'origine e il bucket B è la destinazione. Supponiamo ora di aggiungere un'altra configurazione di replica dove il bucket B è l'origine e il bucket C è la destinazione. In questo caso, gli oggetti nel bucket B che sono repliche di oggetti nel bucket A non vengono replicati nel bucket C.
- Oggetti nel bucket di origine che sono già stati replicati in una destinazione diversa. Se, ad esempio, modifichi il bucket di destinazione in una configurazione della replica esistente, S3 su Outposts non replica di nuovo gli oggetti.
- Oggetti creati con crittografia lato server con chiavi di crittografia fornite dai clienti (SSE-C).
- Aggiornamenti alle risorse secondarie a livello di bucket.

Se, ad esempio, modifichi la configurazione del ciclo di vita o aggiungi una configurazione di notifica nel bucket di origine, tali modifiche non vengono applicate nel bucket di destinazione. Questa funzionalità permette la presenza di configurazioni diverse nei bucket di origine e di destinazione.

- Operazioni eseguite dalla configurazione del ciclo di vita.

Ad esempio, se abiliti una configurazione del ciclo di vita sul bucket di origine e configuri le operazioni di scadenza, S3 su Outposts crea i contrassegni di eliminazione per gli oggetti scaduti nel bucket di origine, ma non replica gli stessi contrassegni nei bucket di destinazione. Per applicare al bucket di origine e a quello di destinazione la stessa configurazione del ciclo di vita, è sufficiente abilitare quest'ultima in entrambi. Per ulteriori informazioni sulla configurazione del ciclo di vita, consulta [Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts](#).

Cosa non è supportato da Replica Amazon S3 su Outposts?

Le seguenti funzionalità Amazon S3 non sono al momento supportate da S3 su Outposts.

- S3 Replication Time Control (S3 RTC). Il controllo del tempo di replica di S3 (S3 RTC) non è supportato perché il traffico di oggetti in Replica Amazon S3 su Outposts viene gestito dalla rete locale (gateway locale). Per informazioni sui gateway locali, consulta la pagina relativa all'[utilizzo dei gateway locali](#) nella Guida per l'utente di AWS Outposts.
- Replica S3 per le operazioni in batch.

Impostazione della replica

Note

Gli oggetti esistenti nel bucket prima della configurazione della regola di replica non vengono replicati automaticamente. In altre parole, Amazon S3 su Outposts non esegue la replica retroattiva di oggetti. Per replicare gli oggetti creati prima della configurazione della replica, puoi utilizzare l'operazione API `CopyObject` per copiarli nello stesso bucket. Dopo la copia, gli oggetti vengono visualizzati come "nuovi" nel bucket e quindi viene loro applicata la configurazione della replica. Per ulteriori informazioni sulla copia di un oggetto, consulta [Copia di un oggetto in un bucket Amazon S3 su Outposts utilizzando AWS SDK per Java](#) e [CopyObject](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Per abilitare la Replica S3 su Outposts, aggiungi una regola di replica al bucket Outposts di origine. La regola di replica indica a S3 su Outposts di replicare gli oggetti come specificato. Nella regola di replica devi fornire le informazioni seguenti:

- Il punto di accesso del bucket Outposts di origine: il nome della risorsa Amazon (ARN) del punto di accesso o l'alias del punto di accesso del bucket dal quale desideri che S3 su Outposts replichi gli oggetti. Per ulteriori informazioni, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).
- Gli oggetti da replicare: puoi replicare tutti gli oggetti presenti nel bucket Outposts di origine o solo una parte di essi. Puoi identificare un sottoinsieme specificando nella configurazione un [prefisso di nome di chiave](#), uno o più tag di oggetti oppure entrambi.

Se, ad esempio, configuri una regola di replica per replicare solo gli oggetti con il prefisso di nome di chiave Tax/, S3 su Outposts replica gli oggetti con chiavi come Tax/doc1 o Tax/doc2. Ma non replica un oggetto con la chiave Legal/doc3. Se specifichi sia un prefisso sia uno o più tag, S3 su Outposts replica solo gli oggetti con il prefisso della chiave e i tag specificati.

- Il bucket Outposts di destinazione: l'ARN o l'alias del punto di accesso del bucket in cui desideri che S3 su Outposts replichi gli oggetti.

Puoi configurare la regola di replica utilizzando la REST API, gli SDK AWS, AWS Command Line Interface (AWS CLI) o la console di Amazon S3.

S3 su Outposts fornisce anche le operazioni API per supportare la configurazione delle regole di replica. Per ulteriori informazioni, consulta i seguenti argomenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [PutBucketReplication](#)
- [GetBucketReplication](#)
- [DeleteBucketReplication](#)

Argomenti

- [Prerequisiti per la creazione delle regole di replica](#)
- [Creazione delle regole di replica su Outposts](#)

Prerequisiti per la creazione delle regole di replica

Argomenti

- [Connessione delle sottoreti Outpost di origine e destinazione](#)
- [Creazione di un ruolo IAM](#)

Connessione delle sottoreti Outpost di origine e destinazione

Affinché il traffico di replica passi dall'Outpost di origine all'Outpost di destinazione tramite il gateway locale, è necessario aggiungere un nuovo percorso per configurare la rete. È necessario connettere gli intervalli di rete dell'instradamento interdominio senza classi (CIDR) dei punti di accesso. Per ogni coppia di punti di accesso, devi configurare questa connessione una sola volta.

Alcuni passaggi per configurare la connessione variano a seconda del tipo di accesso degli endpoint Outposts associati ai punti di accesso. Il tipo di accesso per gli endpoint è Privato (instradamento diretto del cloud privato virtuale [VPC] per AWS Outposts) o IP di proprietà del cliente (un pool di indirizzi IP di proprietà del cliente [pool ColIP] all'interno della rete on-premise).

Passaggio 1: Trovare l'intervallo CIDR dell'endpoint Outposts di origine

Per trovare l'intervallo CIDR dell'endpoint di origine associato al punto di accesso di origine

1. Accedere a Console di gestione AWS e aprire la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Nell'elenco Bucket di Outposts scegli il bucket di origine che desideri per la replica.
4. Scegli la scheda Punti di accesso di Outposts e scegli il punto di accesso di Outposts per il bucket di origine della tua regola di replica.
5. Scegli l'endpoint di Outposts.
6. Copia l'ID della sottorete da utilizzare nel [passaggio 5](#).
7. Il metodo utilizzato per trovare l'intervallo CIDR dell'endpoint di Outposts di origine dipende dal tipo di accesso dell'endpoint.

Nella sezione Panoramica dell'endpoint Outposts, esamina il tipo di accesso.

- Se il tipo di accesso è Privato, copia il valore Instradamento interdominio senza classi (CIDR) da utilizzare nel [passaggio 6](#).
- Se il tipo di accesso è IP di proprietà del cliente, procedi come segue:
 1. Copia il valore del pool IPv4 di proprietà del cliente da utilizzare in seguito come ID del pool di indirizzi.
 2. Apri la console AWS Outposts all'indirizzo <https://console.aws.amazon.com/outposts/>.
 3. Nel riquadro di navigazione, seleziona Tabelle di routing del gateway locale.
 4. Scegli il valore ID tabella di routing del gateway locale dell'Outpost di origine.
 5. Nel riquadro dei dettagli, scegli la scheda Pool ColIP. Incolla il valore dell'ID del pool ColIP che hai copiato in precedenza nella casella di ricerca.
 6. Per il pool ColIP corrispondente, copia il valore CIDR corrispondente dell'endpoint Outposts di origine per utilizzarlo nel [passaggio 6](#).

Passaggio 2: trovare l'ID della sottorete e l'intervallo CIDR dell'endpoint Outposts di destinazione

Per trovare l'ID della sottorete e l'intervallo CIDR dell'endpoint di destinazione associato al punto di accesso di destinazione, segui gli stessi passaggi del [passaggio 1](#) e modifica l'endpoint Outposts di origine con l'endpoint Outposts di destinazione quando esegui i passaggi. Copia il valore dell'ID della sottorete dell'endpoint Outposts di destinazione per utilizzarlo nel [passaggio 6](#). Copia il valore CIDR dell'endpoint Outposts di destinazione per utilizzarlo nel [passaggio 5](#).

Passaggio 3: trovare l'ID del gateway locale dell'Outpost di origine

Per trovare l'ID del gateway locale dell'Outpost di origine

1. Apri la console AWS Outposts all'indirizzo <https://console.aws.amazon.com/outposts/>.
2. Nel riquadro di navigazione a sinistra scegli Gateway locali.
3. Nella pagina Gateway locali trova l'ID dell'Outpost di origine che desideri utilizzare per la replica.
4. Copia il valore dell'ID del gateway locale dell'Outpost di origine per utilizzarlo nel [passaggio 5](#).

Per informazioni sui gateway locali, consulta [Gateway locale](#) nella Guida per l'utente di AWS Outposts.

Passaggio 4: trovare l'ID del gateway locale dell'Outpost di destinazione

Per trovare l'ID del gateway locale dell'Outpost di destinazione, segui gli stessi passaggi del [passaggio 3](#), esclusa la ricerca dell'ID dell'Outpost di destinazione. Copia il valore dell'ID del gateway locale dell'Outpost di destinazione per utilizzarlo nel [passaggio 6](#).

Passaggio 5: configurare la connessione dalla sottorete Outpost di origine alla sottorete Outpost di destinazione

Per configurare la connessione dalla sottorete Outpost di origine alla sottorete Outpost di destinazione

1. Accedi alla Console di gestione AWS e apri la console VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione a sinistra, seleziona Sottoreti.
3. Nella casella di ricerca, inserisci l'ID della sottorete per l'endpoint Outposts di origine che hai individuato nel [passaggio 1](#). Scegli la sottorete con l'ID corrispondente.
4. Per l'elemento della sottorete corrispondente, scegli il valore della Tabella di instradamento di questa sottorete.

5. Nella pagina con una tabella di instradamento selezionata, scegli Operazioni e quindi Modifica instradamenti.
6. Nella scheda Modifica instradamenti scegli Aggiungi routing.
7. In Destinazione, inserisci l'intervallo CIDR dell'endpoint Outposts di destinazione che hai individuato nel [passaggio 2](#).
8. In Destinazione, scegli Gateway locale outpost e inserisci l'ID del gateway locale dell'Outpost di origine che hai individuato nel [passaggio 3](#).
9. Scegli Save changes (Salva modifiche).
10. Assicurati che lo Stato dell'instradamento sia Attivo.

Passaggio 6: configurare la connessione dalla sottorete Outpost di destinazione alla sottorete Outpost di origine

1. Accedi alla Console di gestione AWS e apri la console VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione a sinistra, seleziona Sottoreti.
3. Nella casella di ricerca, inserisci l'ID della sottorete per l'endpoint Outposts di destinazione che hai individuato nel [passaggio 2](#). Scegli la sottorete con l'ID corrispondente.
4. Per l'elemento della sottorete corrispondente, scegli il valore della Tabella di instradamento di questa sottorete.
5. Nella pagina con una tabella di instradamento selezionata, scegli Operazioni e quindi Modifica instradamenti.
6. Nella scheda Modifica instradamenti scegli Aggiungi routing.
7. In Destinazione, inserisci l'intervallo CIDR dell'endpoint Outposts di origine che hai individuato nel [passaggio 1](#).
8. In Destinazione, scegli Gateway locale outpost e inserisci l'ID del gateway locale dell'Outpost di destinazione che hai individuato nel [passaggio 4](#).
9. Scegli Save changes (Salva modifiche).
10. Assicurati che lo Stato dell'instradamento sia Attivo.

Dopo aver collegato gli intervalli di rete CIDR dei punti di accesso di origine e di destinazione, è necessario creare un ruolo AWS Identity and Access Management (IAM).

Creazione di un ruolo IAM

Per impostazione predefinita, tutte le risorse S3 su Outposts, ossia bucket, oggetti e risorse secondarie correlate, sono private e solo il proprietario vi può accedere. S3 su Outposts ha bisogno delle autorizzazioni per leggere e replicare gli oggetti dal bucket Outposts di origine. Queste autorizzazioni vengono concesse creando un ruolo del servizio IAM e specificandolo nella configurazione della replica.

In questa sezione vengono illustrate la policy di trust e la policy di autorizzazione minima richiesta. Le procedure dettagliate di esempio forniscono istruzioni dettagliate per la creazione di un ruolo IAM. Per ulteriori informazioni, consulta [Creazione delle regole di replica su Outposts](#). Per ulteriori informazioni sui ruoli IAM, consulta [Ruoli IAM](#) nella Guida per l'utente di IAM.

- Di seguito viene mostrata una policy di attendibilità in cui identifichi S3 su Outposts come principale del servizio che può assumere il ruolo.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "s3-outposts.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

- Di seguito viene mostrata una policy di accesso in cui concedi al ruolo le autorizzazioni per eseguire attività di replica per tuo conto. Quando S3 su Outposts assume il ruolo, dispone delle autorizzazioni che sono state specificate in questa policy. Per utilizzare questa policy, sostituisci **user input placeholders** con le tue specifiche informazioni. Assicurati di sostituirle con gli ID degli Outpost di origine e di destinazione, i nomi dei bucket e i nomi dei punti di accesso dei bucket Outposts di origine e di destinazione.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "s3-outposts.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

```

"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/*"
    ]
  }
]
}

```

La policy di accesso concede le autorizzazioni per le seguenti operazioni:

- `s3-outposts:GetObjectVersionForReplication`: l'autorizzazione per questa operazione viene concessa a tutti gli oggetti per consentire a S3 su Outposts di ottenere una versione specifica dell'oggetto associata a ciascun oggetto.
- `s3-outposts:GetObjectVersionTagging`: l'autorizzazione per questa operazione sugli oggetti nel bucket **SOURCE-OUTPOSTS-BUCKET** (bucket di origine) permettono a S3 su Outposts di leggere i tag degli oggetti per la replica. Per ulteriori informazioni, consulta [Aggiunta di tag](#)

[per bucket S3 su Outposts](#). Se S3 su Outposts non dispone di questa autorizzazione, replica gli oggetti ma non i relativi tag.

- `s3-outposts:ReplicateObject` e `s3-outposts:ReplicateDelete`: le autorizzazioni per queste operazioni sugli oggetti nel bucket **DESTINATION-OUTPOSTS-BUCKET** (il bucket di destinazione) permettono a S3 su Outposts di replicare gli oggetti o eliminare i contrassegni nel bucket Outposts di destinazione. Per informazioni sui contrassegni di eliminazione, consulta la sezione [Effetto delle operazioni di eliminazione sulla replica](#).

Note

- Le autorizzazioni per l'operazione `s3-outposts:ReplicateObject` nel bucket **DESTINATION-OUTPOSTS-BUCKET** (il bucket di destinazione) consentono anche la replica dei tag degli oggetti. Pertanto non è necessario concedere esplicitamente l'autorizzazione per l'operazione `s3-outposts:ReplicateTags`.
- Per la replica tra account, il proprietario del bucket Outposts di destinazione deve aggiornare la policy dei bucket per concedere l'autorizzazione per l'operazione `s3-outposts:ReplicateObject` nel **DESTINATION-OUTPOSTS-BUCKET**. L'operazione `s3-outposts:ReplicateObject` consente a S3 su Outposts di replicare oggetti e tag nel bucket Outposts di destinazione.

Per un elenco delle operazioni di S3 on Outposts, consulta [Operazioni definite da Amazon S3 su Outposts](#).

Important

L'Account AWS che possiede il ruolo IAM deve disporre delle autorizzazioni per le operazioni che concede al ruolo.

Supponi ad esempio che il bucket Outposts di origine contenga oggetti di proprietà di un altro Account AWS. Occorre che il proprietario degli oggetti conceda esplicitamente le autorizzazioni richieste all'Account AWS proprietario del ruolo IAM tramite la policy dei bucket e la policy dei punti di accesso. In caso contrario, S3 su Outposts non può accedere agli oggetti e la replica degli oggetti ha esito negativo.

Le autorizzazioni descritte si riferiscono alla configurazione di replica minima. Se scegli di aggiungere configurazioni di replica facoltative, devi concedere ulteriori autorizzazioni a S3 su Outposts.

Concessione di autorizzazioni quando i bucket Outposts di origine e di destinazione sono di proprietà di Account AWS diversi

Quando i bucket Outposts di origine e di destinazione non sono di proprietà degli stessi account, il proprietario del bucket Outposts di destinazione deve aggiornare le policy dei bucket e dei punti di accesso per il bucket di destinazione. Queste policy devono concedere al proprietario del bucket Outposts di origine e al ruolo del servizio IAM le autorizzazioni per eseguire le operazioni di replica, come mostrato nei seguenti esempi di policy. In caso contrario la replica avrà esito negativo. In questi esempi di policy, **DESTINATION-OUTPOSTS-BUCKET** è il bucket di destinazione. Per usare questi esempi di policy, sostituisci **user input placeholders** con le tue informazioni.

Se stai creando il ruolo di servizio IAM manualmente, imposta il percorso del ruolo come `role/service-role/`, nel modo mostrato nei seguenti esempi di policy. Per ulteriori informazioni, consulta [ARN IAM](#) nella Guida per l'utente di 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-1:44445556666: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/*"  
            ]  
        }  
    ]  
}
```

i Note

In presenza di oggetti con tag nel bucket Outposts di origine, tenere in considerazione quanto segue:

Se il proprietario del bucket Outposts di origine concede a S3 su Outposts l'autorizzazione per le operazioni `s3-outposts:GetObjectVersionTagging` e `s3-outposts:ReplicateTags` per replicare i tag degli oggetti (tramite il ruolo IAM), Amazon S3 replica i tag insieme agli oggetti. Per informazioni sul ruolo IAM, consulta [Creazione di un ruolo IAM](#).

Creazione delle regole di replica su Outposts

La Replica S3 su Outposts è la copia asincrona e automatica degli oggetti di vari bucket negli stessi o in diversi AWS Outposts. Il processo replica gli oggetti appena creati e gli aggiornamenti degli oggetti da un bucket Outposts di origine in uno o più bucket Outposts di destinazione. Per ulteriori informazioni, consulta [Replica degli oggetti per S3 su Outposts](#).

Note

Gli oggetti esistenti nel bucket Outposts di origine prima della configurazione delle regole di replica non vengono replicati. In altre parole, S3 su Outposts non esegue la replica degli oggetti in modo retroattivo. Per replicare gli oggetti creati prima della configurazione della replica, puoi utilizzare l'operazione API `CopyObject` per copiarli nello stesso bucket. Dopo la copia, gli oggetti vengono visualizzati come "nuovi" nel bucket e quindi viene loro applicata la configurazione della replica. Per ulteriori informazioni sulla copia di un oggetto, consulta [Copia di un oggetto in un bucket Amazon S3 su Outposts utilizzando AWS SDK per Java](#) e [CopyObject](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Quando si configura la replica, vengono aggiunte le regole di replica al bucket Outposts di origine. Le regole di replica definiscono gli oggetti del bucket Outposts di origine da replicare e i bucket Outposts di destinazione in cui vengono archiviati gli oggetti replicati. È possibile creare una regola per replicare tutti gli oggetti in un bucket o un sottoinsieme di oggetti con un prefisso di nome di chiave specifico, uno o più tag di oggetto o entrambi gli elementi. Un bucket Outposts di destinazione può trovarsi nello stesso Outpost del bucket Outposts di origine o in un Outpost diverso.

Per le regole di replica di S3 su Outposts, devi fornire il nome della risorsa Amazon (ARN) del punto di accesso del bucket Outposts di origine e il nome della risorsa Amazon (ARN) del punto di accesso del bucket Outposts di destinazione anziché i nomi dei bucket Outposts di origine e di destinazione.

Se specifichi l'ID della versione dell'oggetto da eliminare, S3 su Outposts elimina la versione dell'oggetto nel bucket Outposts di origine. Tuttavia non replica l'eliminazione nel bucket Outposts di destinazione. In altre parole, non elimina la stessa versione dell'oggetto dal bucket Outposts di destinazione. Questo comportamento permette di proteggere i dati da eliminazioni da parte di utenti malintenzionati.

Quando si aggiunge una regola di replica a un bucket Outposts, la regola viene abilitata per impostazione predefinita e pertanto inizia a funzionare non appena viene salvata.

In questo esempio viene configurata la replica per i bucket Outposts di origine e di destinazione in Outpost diversi e di proprietà dello stesso Account AWS. Sono forniti esempi per utilizzare la console di Amazon S3, la AWS Command Line Interface (AWS CLI) e AWS SDK per Java e AWS SDK per .NET. Per ulteriori informazioni sulle autorizzazioni della Replica S3 su Outposts tra account, consulta [Concessione di autorizzazioni quando i bucket Outposts di origine e di destinazione sono di proprietà di Account AWS diversi](#).

Per i prerequisiti per configurare le regole di replica di S3 su Outposts, consulta [Prerequisiti per la creazione delle regole di replica](#).

Utilizzo della console S3

Segui questi passaggi per configurare una regola di replica quando il bucket Amazon S3 su Outposts di destinazione si trova in un Outpost diverso rispetto al bucket Outposts di origine.

Se il bucket Outposts di destinazione si trova in un account diverso rispetto al bucket Outposts di origine, è necessario aggiungere al bucket Outposts di destinazione una policy dei bucket per fornire al proprietario dell'account del bucket Outposts di origine l'autorizzazione per replicare gli oggetti nel bucket Outposts di destinazione.

Per creare una regola di replica

1. Accedere a Console di gestione AWS e aprire la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nell'elenco Bucket Outposts scegli il nome del bucket che desideri utilizzare come bucket di origine.
3. Seleziona la scheda Gestione, scorri verso il basso fino a Regole di replica e quindi scegli Crea regola di replica.
4. In Nome della regola di replica specifica un nome per la regola al fine di poterla identificare in un secondo momento. Il nome è obbligatorio e deve essere univoco all'interno del bucket.
5. In Stato, l'opzione Abilitato è selezionata per impostazione predefinita. Una regola abilitata inizia a funzionare non appena viene salvata. Se desideri abilitare la regola in un secondo momento, seleziona Disabilitata.
6. In Priorità, il valore di priorità della regola determina quale regola viene applicata in caso di sovrapposizione delle regole. Quando gli oggetti sono inclusi nell'ambito di più regole di replica, S3 su Outposts utilizza questi valori di priorità per evitare i conflitti. Per impostazione predefinita, le nuove regole vengono aggiunte alla configurazione di replica con la priorità più alta. Più elevato è il numero, maggiore è la priorità.

Per modificare la priorità della regola, dopo averla salvata, scegli il nome della regola dall'elenco delle regole di replica, seleziona Operazioni e quindi scegli Modifica priorità.

7. In Bucket di origine sono disponibili le seguenti opzioni per l'impostazione dell'origine della replica:

- Per replicare l'intero bucket, scegli Applica a tutti gli oggetti nel bucket.
- Per applicare il filtro di prefisso o tag all'origine di replica, scegli Limita l'ambito della regola utilizzando uno o più filtri. È possibile combinare un prefisso con i tag.
 - Per replicare tutti gli oggetti con lo stesso prefisso, immetti un prefisso nella casella Prefisso. Con il filtro Prefisso limita la replica a tutti gli oggetti con nomi che iniziano con la stessa stringa (ad esempio, *pictures*).

Se immetti un prefisso corrispondente al nome di una cartella, devi utilizzare una / (barra) come ultimo carattere (ad esempio, *pictures/*).

- Per replicare tutti gli oggetti contenenti uno o più tag di oggetto, seleziona Aggiungi tag e specifica la coppia valore-chiave nelle caselle. Per aggiungere un altro tag, ripeti la procedura. Per ulteriori informazioni sui tag degli oggetti, consulta [Aggiunta di tag per bucket S3 su Outposts](#).

8. Per accedere al bucket di origine S3 su Outposts per la replica, in Nome del punto di accesso di origine, scegli un punto di accesso associato al bucket di origine.

9. In Destinazione, scegli il nome della risorsa Amazon (ARN) del punto di accesso del bucket Outposts di destinazione in cui desideri che S3 su Outposts replichi gli oggetti. I bucket Outposts di destinazione possono trovarsi nello stesso o in diversi Account AWS del bucket Outposts di origine.

Se il bucket di destinazione si trova in un account diverso rispetto al bucket Outposts di origine, è necessario aggiungere al bucket Outposts di destinazione una policy del bucket per fornire al proprietario dell'account del bucket Outposts di origine l'autorizzazione per replicare gli oggetti nel bucket Outposts di destinazione. Per ulteriori informazioni, consulta [Concessione di autorizzazioni quando i bucket Outposts di origine e di destinazione sono di proprietà di Account AWS diversi](#).

Note

Se la funzione Controllo delle versioni non è abilitata nel bucket Outposts di destinazione, viene visualizzato un messaggio di avviso contenente un pulsante Abilita

Controllo delle versioni. Seleziona questo pulsante per abilitare la funzione Controllo delle versioni nel bucket.

10. Configura un ruolo di servizio AWS Identity and Access Management (IAM) che S3 su Outposts può assumere per replicare gli oggetti per tuo conto.

Per impostare un ruolo IAM, in Ruolo IAM effettua una delle operazioni seguenti:

- Per fare in modo che S3 su Outposts crei un nuovo ruolo IAM per la configurazione di replica, seleziona Scegli tra i ruoli IAM esistenti e quindi Crea nuovo ruolo. Quando salvi la regola, viene generata una nuova policy per il ruolo IAM corrispondente ai bucket Outposts di origine e di destinazione scelti. Consigliamo di scegliere Crea nuovo ruolo.
- Puoi anche decidere di utilizzare un ruolo IAM esistente. In tal caso, è necessario scegliere un ruolo che conceda a S3 su Outposts le autorizzazioni necessarie per la replica. Se questo ruolo non concede autorizzazioni sufficienti a S3 su Outposts per seguire la regola di replica, la replica non riesce.

Per scegliere un ruolo esistente, seleziona Scegli tra i ruoli IAM esistenti e scegli il ruolo nel menu a discesa. Puoi anche scegliere Inserisci l'ARN del ruolo IAM e quindi inserire il nome della risorsa Amazon (ARN) del ruolo IAM.

⚠ Important

Quando aggiungi una regola di replica a un bucket S3 su Outposts, è necessario disporre delle autorizzazioni `iam:CreateRole` e `iam:PassRole` per poter creare e trasferire il ruolo IAM che concede le autorizzazioni di replica a S3 su Outposts. Per ulteriori informazioni, consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a un Servizio AWS](#) nella Guida per l'utente di IAM.

11. Tutti gli oggetti nei bucket Outposts sono crittografati per impostazione predefinita. Per ulteriori informazioni sulla crittografia di S3 su Outposts, consulta [Crittografia dei dati in S3 su Outposts](#). È possibile replicare solo gli oggetti crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3). La replica degli oggetti crittografati utilizzando la crittografia lato server con le chiavi AWS Key Management Service (AWS KMS) (SSE-KMS) o la crittografia lato server con le chiavi di crittografia fornite dal cliente (SSE-C) non è supportata.
12. Se necessario, abilita le seguenti opzioni aggiuntive durante l'impostazione della configurazione della regola di replica:

- Se desideri abilitare i parametri della replica S3 su Outposts nella configurazione di replica, seleziona Parametri di replica. Per ulteriori informazioni, consulta [Monitoraggio dell'avanzamento con le metriche relative alla replica](#).
- Se desideri abilitare la replica del contrassegno di eliminazione nella configurazione di replica, seleziona Replica del contrassegno di eliminazione. Per ulteriori informazioni, consulta [Effetto delle operazioni di eliminazione sulla replica](#).
- Se desideri replicare le modifiche ai metadati apportate alle repliche negli oggetti di origine, seleziona Sincronizzazione delle modifiche delle repliche. Per ulteriori informazioni, consulta [Stato della replica se su Outposts è abilitata la sincronizzazione della modifica della replica Amazon S3](#).

13. Per finire, scegli Crea regola.

Dopo aver salvato la regola, è possibile modificarla, abilitarla, disabilitarla o eliminarla. Per eseguire queste operazioni, vai alla scheda Gestione del bucket Outposts di origine, scorri verso il basso fino alla sezione Regole di replica, scegli la tua regola e quindi scegli Modifica regola.

Utilizzando AWS CLI

Per utilizzare la AWS CLI per impostare la replica quando i bucket Outposts di origine e di destinazione sono di proprietà dello stesso Account AWS, esegui le seguenti operazioni:

- Crea i bucket Outposts di origine e di destinazione.
- Abilita il controllo delle versioni su entrambi i bucket.
- Crea un ruolo IAM che permette a S3 su Outposts di replicare gli oggetti.
- Aggiungi la configurazione di replica al bucket Outposts di origine.

Per verificare l'impostazione, testarla.

Per impostare la replica quando i bucket Outposts di origine e di destinazione sono di proprietà dello stesso Account AWS

1. Impostare un profilo di credenziali per la AWS CLI, utilizzando il nome profilo acctA. Per informazioni sull'impostazione di profili con credenziali, consulta [Profilo denominato](#) nella Guida per l'utente di AWS Command Line Interface.

Important

Il profilo utilizzato per questo esercizio deve disporre delle autorizzazioni necessarie. Ad esempio, nella configurazione di replica dovrai specificare il ruolo di servizio IAM che S3 su Outposts può assumere. Puoi effettuare questa operazione solo se il profilo che utilizzi dispone delle autorizzazioni `iam:CreateRole` e `iam:PassRole`. Per ulteriori informazioni, consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a un Servizio AWS](#) nella Guida per l'utente di IAM. Se utilizzi le credenziali di amministratore per creare un profilo denominato, il profilo denominato avrà le autorizzazioni necessarie per eseguire tutte le attività.

2. Creare un bucket di origine e abilitare la funzione Controllo delle versioni. Il comando `create-bucket` seguente crea un bucket **SOURCE-OUTPOSTS-BUCKET** nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1). Per utilizzare questo comando, sostituisci **user input placeholders** con le tue specifiche informazioni.

```
aws s3control create-bucket --bucket SOURCE-OUTPOSTS-BUCKET --outpost-id SOURCE-OUTPOST-ID --profile acctA --region us-east-1
```

Il comando `put-bucket-versioning` seguente abilita il controllo delle versioni sul bucket **SOURCE-OUTPOSTS-BUCKET**. Per utilizzare questo comando, sostituisci **user input placeholders** con le tue specifiche informazioni.

```
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. Creare un bucket di destinazione e abilitare la funzione Controllo delle versioni. Il comando `create-bucket` seguente crea un bucket **DESTINATION-OUTPOSTS-BUCKET** nella regione Stati Uniti occidentali (Oregon) (us-west-2). Per utilizzare questo comando, sostituisci **user input placeholders** con le tue specifiche informazioni.

Note

Per impostare la configurazione di replica quando entrambi i bucket Outposts di origine e di destinazione si trovano nello stesso Account AWS si utilizza lo stesso profilo denominato. Questo esempio utilizza `acctA`. Per testare la configurazione della replica

quando i bucket sono di proprietà di Account AWS diversi, occorre specificare profili differenti per ciascun bucket.

```
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
```

Il comando `put-bucket-versioning` seguente abilita il controllo delle versioni sul bucket **DESTINATION-OUTPOSTS-BUCKET**. Per utilizzare questo comando, sostituisci *user input placeholders* con le tue specifiche informazioni.

```
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. Crea un ruolo di servizio IAM. Aggiungi questo ruolo di servizio al bucket **SOURCE-OUTPOSTS-BUCKET** in un secondo momento nella configurazione di replica. S3 su Outposts assume questo ruolo per replicare gli oggetti per tuo conto. Il ruolo IAM si crea in due fasi:
 - a. Creare un ruolo IAM.

- i. Copiare la seguente policy di attendibilità e salvarla in un file denominato `s3-on-outposts-role-trust-policy.json` nella directory corrente sul computer locale. Questa policy fornisce a S3 su Outposts le autorizzazioni ai principali del servizio per assumere il ruolo di servizio.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3-outposts.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```

    ]
}
```

- ii. Per creare un ruolo, esegui il comando seguente. Sostituire *user input placeholders* con le proprie informazioni.

```
aws iam create-role --role-name replicationRole --assume-role-policy-document file://s3-on-outposts-role-trust-policy.json --profile acctA
```

- b. Collega una policy di autorizzazioni al ruolo di servizio.

- i. Copiare la seguente policy di autorizzazioni e salvarla in un file denominato `s3-on-outposts-role-permissions-policy.json` nella directory corrente sul computer locale. Questa policy fornisce le autorizzazioni per varie operazioni su oggetti e bucket S3 su Outposts. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue specifiche informazioni.

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. Eseguire il comando seguente per creare una policy e collegarla al ruolo. Sostituire *user input placeholders* con le proprie informazioni.

```
aws iam put-role-policy --role-name replicationRole --policy-document file://s3-on-outposts-role-permissions-policy.json --policy-name replicationRolePolicy --profile accta
```

5. Aggiungi la configurazione di replica al bucket **SOURCE-OUTPOSTS-BUCKET**.

- a. Anche se l'API S3 su Outposts richiede la configurazione di replica in formato XML, la AWS CLI richiede di specificare la configurazione di replica in formato JSON. Salvare il seguente JSON in un file denominato `replication.json` nella directory locale sul computer in uso. Per utilizzare questa configurazione, sostituisci *user input placeholders* con le tue specifiche informazioni.

```
{
    "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. Esegui il comando `put-bucket-replication` seguente per aggiungere la configurazione di replica al bucket Outposts di origine. Per utilizzare questo comando, sostituisci `user input placeholders` con le tue specifiche informazioni.

```
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. Per recuperare la configurazione di replica, utilizzare il comando `get-bucket-replication`. Per utilizzare questo comando, sostituisci `user input placeholders` con le tue specifiche informazioni.

```
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. Verifica la configurazione nella console di Amazon S3:

- Accedi alla Console di gestione AWS e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
- Nel bucket di `SOURCE-OUTPOSTS-BUCKET`, crea una cartella denominata Tax.
- Aggiungi oggetti di esempio alla cartella Tax del bucket di `SOURCE-OUTPOSTS-BUCKET`.
- Nel bucket di `DESTINATION-OUTPOSTS-BUCKET`, verifica quanto segue:
 - S3 su Outposts ha replicato gli oggetti.

 Note

Il tempo richiesto da S3 su Outposts per la replica di un oggetto dipende dalle dimensioni dell'oggetto. Per informazioni su come visualizzare lo stato della replica, consulta la sezione [Ottenimento delle informazioni sullo stato della replica](#).

- Nella scheda Proprietà dell'oggetto, lo Stato di replica è impostato su Replica (che identifica l'oggetto come replica).

Gestione della replica

In questa sezione vengono descritte ulteriori opzioni per la configurazione della replica disponibili in S3 su Outposts, nonché viene spiegato come determinare lo stato della replica e come risolvere i problemi della replica. Per informazioni sulla configurazione della replica di base, consulta [Impostazione della replica](#).

Argomenti

- [Monitoraggio dell'avanzamento con le metriche relative alla replica](#)
- [Ottenimento delle informazioni sullo stato della replica](#)
- [Risoluzione dei problemi nella replica](#)
- [Utilizzo di EventBridge per la replica S3 su Outposts](#)

Monitoraggio dell'avanzamento con le metriche relative alla replica

Replica Amazon S3 su Outposts fornisce metriche dettagliate per le regole di replica nella configurazione della replica. Con le metriche relative alla replica puoi monitorare l'avanzamento della replica a intervalli di 5 minuti tramite il tracciamento dei byte in attesa di replica, della latenza della replica e delle operazioni in attesa di replica. A supporto della procedura di risoluzione dei problemi relativi alla configurazione, puoi anche configurare Amazon EventBridge in modo da ricevere notifiche relative agli errori di replica.

Se le metriche di replica sono abilitate, Replica Amazon S3 su Outposts pubblicano le seguenti metriche su Amazon CloudWatch:

- Byte in attesa di replica: il numero totale di byte di oggetti in attesa di replica per una determinata regola di replica.
- Latenza di replica: il numero massimo di secondi entro i quali i bucket di destinazione della replica sono in ritardo rispetto al bucket di origine per una determinata regola di replica.
- Operazioni in attesa di replica: il numero di operazioni in attesa di replica per una determinata regola di replica. Le operazioni includono oggetti, contrassegni di eliminazione e tag.

Note

Le metriche di Replica Amazon S3 su Outposts vengono fatturate alla stessa tariffa delle metriche personalizzate di Amazon CloudWatch. Per ulteriori informazioni, consultare la pagina dei [prezzi di CloudWatch](#)

Ottenimento delle informazioni sullo stato della replica

Lo stato della replica consente di determinare lo stato corrente di un oggetto sottoposto a replica in Amazon S3 su Outposts. Lo stato della replica di un oggetto di origine restituirà PENDING, COMPLETED o FAILED. Lo stato della replica di una replica restituirà REPLICA.

Panoramica dello stato della replica

In uno scenario di replica, esistono un bucket di origine in cui si configura la replica e un bucket di destinazione in cui S3 su Outposts replica gli oggetti. Quando richiedi un oggetto (tramite `GetObject`) o i metadati di un oggetto (tramite `HeadObject`) da questi bucket, S3 su Outposts restituisce l'intestazione `x-amz-replication-status` nella risposta come segue:

- Quando richiedi un oggetto dal bucket di origine, S3 su Outposts restituisce l'intestazione `x-amz-replication-status` se l'oggetto nella richiesta è idoneo per la replica.

Supponiamo, ad esempio, che nella configurazione della replica venga specificato il prefisso di oggetto `TaxDocs` che indica a S3 su Outposts di replicare solo gli oggetti con il prefisso del nome della chiave `TaxDocs`. Tutti gli oggetti caricati che hanno questo prefisso del nome della chiave, ad esempio `TaxDocs/document1.pdf`, verranno replicati. Per le richieste di oggetti con questo prefisso del nome della chiave, S3 su Outposts restituisce l'intestazione `x-amz-replication-status` con uno dei valori seguenti per lo stato della replica dell'oggetto: PENDING, COMPLETED o FAILED.

Note

Se la replica dell'oggetto ha esito negativo dopo il caricamento di un oggetto, non è possibile provare a eseguirla di nuovo. È necessario caricare di nuovo l'oggetto. Gli oggetti passano a uno stato FAILED per problemi dovuti ad esempio alla mancanza di autorizzazioni per il ruolo di replica o autorizzazioni di bucket mancanti. In caso di errori temporanei, ad esempio se un bucket o un outpost non è disponibile, lo stato della replica

non passerà a FAILED, ma rimarrà PENDING. Dopo che la risorsa è tornata online, S3 su Outposts riprenderà la replica di tali oggetti.

- Quando richiedi un oggetto da un bucket di destinazione, se l'oggetto nella richiesta è una replica creata da S3 su Outposts, S3 su Outposts restituisce l'intestazione `x-amz-replication-status` con il valore REPLICA.

Note

Prima di eliminare un oggetto da un bucket di origine in cui è abilitata la replica, è consigliabile controllare lo stato della replica per assicurarsi che l'oggetto sia stato replicato.

Stato della replica se su Outposts è abilitata la sincronizzazione della modifica della replica Amazon S3

Quando le regole di replica abilitano la sincronizzazione delle modifiche della replica S3 su Outposts, le repliche possono riportare stati diversi da REPLICA. Se le modifiche dei metadati sono in corso di replica, l'intestazione `x-amz-replication-status` della replica restituisce PENDING. Se la sincronizzazione delle modifiche della replica non riesce a replicare i metadati, l'intestazione della replica restituisce FAILED. Se i metadati vengono replicati correttamente, l'intestazione della replica restituisce il valore REPLICA.

Risoluzione dei problemi nella replica

Se le repliche degli oggetti non vengono visualizzate nel bucket Amazon S3 su Outposts di destinazione dopo aver configurato la replica, usa questi suggerimenti per identificare e risolvere i problemi.

- Il tempo impiegato da S3 su Outposts per replicare un oggetto dipende da diversi fattori, tra cui la distanza tra gli outpost di origine e destinazione e le dimensioni dell'oggetto.

È possibile controllare lo stato della replica dell'oggetto di origine. Se lo stato della replica dell'oggetto è PENDING, significa che S3 su Outposts non ha completato la replica. Se lo stato della replica dell'oggetto è FAILED, controlla la configurazione della replica impostata nel bucket di origine.

- Nella configurazione di replica nel bucket di origine verifica quanto segue:

- La correttezza del nome della risorsa Amazon (ARN) del punto di accesso relativo al bucket di destinazione.
- La correttezza del prefisso del nome della chiave. Ad esempio, se si imposta la configurazione per replicare gli oggetti con il prefisso Tax, solo gli oggetti con i nomi della chiave quali Tax/document1 o Tax/document2 vengono replicati. Un oggetto con il nome della chiave document3 non sia replicato.
- Che lo stato sia Enabled.
- Verifica che il controllo delle versioni non sia stato sospeso per nessuno dei bucket. Sia per il bucket di origine che per quello di destinazione deve essere abilitata la funzione Controllo delle versioni.
- Se il bucket di destinazione è di proprietà di un altro Account AWS, verifica che il proprietario di tale bucket disponga di una policy del bucket che consenta al proprietario del bucket di origine di replicare gli oggetti. Per un esempio, consulta [Concessione di autorizzazioni quando i bucket Outposts di origine e di destinazione sono di proprietà di Account AWS diversi](#).
- Se la replica di un oggetto non è presente nel bucket di destinazione, il problema potrebbe essere dovuto alle cause seguenti:
 - S3 su Outposts non replica un oggetto in un bucket di origine che è una replica creata da un'altra configurazione della replica. Se, ad esempio, imposti una configurazione della replica dal bucket A al bucket B al bucket C, S3 su Outposts non replica le repliche degli oggetti del bucket B nel bucket C.

Se desideri replicare gli oggetti del bucket A nel bucket B e nel bucket C, imposta più destinazioni di bucket in regole di replica diverse per la configurazione della replica del bucket di origine. Ad esempio, crea due regole di replica sul bucket di origine A, con una regola da replicare nel bucket di destinazione B e l'altra regola da replicare nel bucket di destinazione C.

- Il proprietario di un bucket di origine può concedere ad altri Account AWS l'autorizzazione necessaria per caricare gli oggetti. Per impostazione predefinita, il proprietario del bucket di origine non dispone di autorizzazioni per gli oggetti creati da altri account. La configurazione di replica esegue la replica solo degli oggetti per i quali il proprietario del bucket di origine dispone delle autorizzazioni di accesso. Per evitare problemi di replica, il proprietario del bucket di origine può concedere ad altri Account AWS le autorizzazioni necessarie per creare oggetti in modo condizionale, richiedendo autorizzazioni di accesso esplicite su quegli oggetti.
- Supponiamo di aggiungere nella configurazione della replica una regola per replicare un sottoinsieme di oggetti con un tag specifico. In questo caso, è necessario assegnare il valore e la chiave del tag specifici al momento della creazione dell'oggetto per permettere a S3 su Outposts di

replicare l'oggetto. Se prima crei un oggetto e quindi aggiungi il tag a tale oggetto, S3 su Outposts non replica l'oggetto.

- La replica non riesce se la policy del bucket nega l'accesso al ruolo di replica per una delle seguenti operazioni:

Bucket di origine:

```
"s3-outposts:GetObjectVersionForReplication",  
"s3-outposts:GetObjectVersionTagging"
```

Bucket di destinazione:

```
"s3-outposts:ReplicateObject",  
"s3-outposts:ReplicateDelete",  
"s3-outposts:ReplicateTags"
```

- Amazon EventBridge può avvisarti quando gli oggetti non vengono replicati negli outpost di destinazione. Per ulteriori informazioni, consulta [Utilizzo di EventBridge per la replica S3 su Outposts](#).

Utilizzo di EventBridge per la replica S3 su Outposts

Amazon S3 su Outposts è integrato con Amazon EventBridge e utilizza lo spazio dei nomi s3-outposts. EventBridge è un servizio routing di eventi serverless che puoi utilizzare per connettere le applicazioni ai dati provenienti da un'ampia gamma di origini. Per ulteriori informazioni, consulta [Che cos'è Amazon EventBridge?](#) nella Guida per l'utente di Amazon EventBridge.

A supporto delle procedure di risoluzione dei problemi relativi alla configurazione della replica, puoi configurare Amazon EventBridge in modo da ricevere le notifiche relative agli eventi di errore relativi alla replica. EventBridge può inviare una notifica quando gli oggetti non vengono replicati nell'istanza Outposts di destinazione. Per ulteriori informazioni sullo stato corrente di un oggetto da replicare, consulta [Panoramica dello stato della replica](#).

Amazon S3 può inviare eventi a EventBridge ogni volta che determinati eventi si verificano nel bucket Outposts. A differenza di altre destinazioni, non è necessario selezionare i tipi di eventi che si desidera inviare. È anche possibile utilizzare le regole di EventBridge per instradare gli eventi a destinazioni aggiuntive. Dopo aver abilitato EventBridge, S3 su Outposts invia tutti i seguenti eventi a EventBridge.

Tipo di evento	Descrizione	Spazio dei nomi
OperationFailedReplication	<p>La replica di un oggetto all'interno di una regola di replica non è riuscita. Per ulteriori informazioni sui motivi degli errori della replica S3 su Outposts, consulta Utilizzo di EventBridge per visualizzare i motivi degli errori della replica S3 su Outposts.</p>	s3-outposts

Utilizzo di EventBridge per visualizzare i motivi degli errori della replica S3 su Outposts

La seguente tabella elenca i motivi degli errori di replica in S3 su Outposts. È possibile configurare una regola di EventBridge per pubblicare e visualizzare il motivo dell'errore tramite Amazon Simple Queue Service (Amazon SQS), Servizio di notifica semplice Amazon (Amazon SNS), AWS Lambda o File di log Amazon CloudWatch. Per ulteriori informazioni sulle autorizzazioni richieste per utilizzare queste risorse per EventBridge, consulta l'argomento relativo all'[uso delle policy basate su risorse per Amazon EventBridge](#).

Motivo dell'errore di replica	Descrizione
AssumeRoleNotPermitted	S3 su Outposts non può assumere il ruolo AWS Identity and Access Management (IAM) specificato nella configurazione della replica.
DstBucketNotFound	S3 su Outposts non è in grado di trovare il bucket di destinazione specificato nella configurazione della replica.
DstBucketUnversioned	Il controllo delle versioni non è abilitato nel bucket Outposts di destinazione. Per replicare gli oggetti con Replica Amazon S3 su Outposts, devi abilitare il controllo delle versioni nel bucket di destinazione.
DstDeleteObjNotPermitted	S3 su Outposts non è in grado di replicare le eliminazioni nel bucket di destinazione. È

Motivo dell'errore di replica	Descrizione
	possibile che manchi l'autorizzazione s3-outposts:ReplicateDelete per il bucket di destinazione.
DstMultipartCompleteNotPermitted	S3 su Outposts non è in grado di completare il caricamento degli oggetti in più parti nel bucket di destinazione. È possibile che manchi l'autorizzazione s3-outposts:ReplicateObject per il bucket di destinazione.
DstMultipartInitNotPermitted	S3 su Outposts non è in grado di avviare il caricamento degli oggetti in più parti nel bucket di destinazione. È possibile che manchi l'autorizzazione s3-outposts:ReplicateObject per il bucket di destinazione.
DstMultipartPartUploadNotPermitted	S3 su Outposts non è in grado di eseguire il caricamento degli oggetti in più parti nel bucket di destinazione. È possibile che manchi l'autorizzazione s3-outposts:ReplicateObject per il bucket di destinazione.
DstOutOfCapacity	S3 su Outposts non è in grado di eseguire la replica nell'outpost di destinazione perché è stata esaurita la capacità di archiviazione S3.
DstPutObjNotPermitted	S3 su Outposts non è in grado di replicare gli oggetti nel bucket di destinazione. È possibile che manchi l'autorizzazione s3-outposts:ReplicateObject per il bucket di destinazione.

Motivo dell'errore di replica	Descrizione
DstPutTaggingNotPermitted	S3 su Outposts non è in grado di replicare tag di oggetti nel bucket di destinazione. È possibile che manchi l'autorizzazione <code>s3-outposts:ReplicateObject</code> per il bucket di destinazione.
DstVersionNotFound	S3 su Outposts non è in grado di trovare la versione dell'oggetto richiesta nel bucket di destinazione per replicare i metadati di tale versione.
SrcBucketReplicationConfigMissing	S3 su Outposts non è in grado di trovare una configurazione della replica per il punto di accesso associato al bucket Outposts di origine.
SrcGetObjNotPermitted	S3 su Outposts non è in grado di accedere all'oggetto nel bucket di origine per la replica. È possibile che manchi l'autorizzazione <code>s3-outposts:GetObjectVersionForReplication</code> per il bucket di origine.
SrcGetTaggingNotPermitted	S3 su Outposts non è in grado di accedere alle informazioni sui tag degli oggetti dal bucket di origine. È possibile che manchi l'autorizzazione <code>s3-outposts:GetObjectVersionTagging</code> per il bucket di origine.
SrcHeadObjectNotPermitted	S3 su Outposts non è in grado di recuperare i metadati degli oggetti dal bucket di origine. È possibile che manchi l'autorizzazione <code>s3-outposts:GetObjectVersionForReplication</code> per il bucket di origine.

Motivo dell'errore di replica	Descrizione
SrcObjectNotEligible	L'oggetto non è idoneo per la replica. L'oggetto o i relativi tag non corrispondono alla configurazione della replica.

Per ulteriori informazioni sulla risoluzione dei problemi relativi alla replica, consulta i seguenti argomenti:

- [Creazione di un ruolo IAM](#)
- [Risoluzione dei problemi nella replica](#)

Monitoraggio di EventBridge con CloudWatch

Per il monitoraggio Amazon EventBridge è integrato con Amazon CloudWatch. EventBridge invia automaticamente le metriche a CloudWatch a intervalli di un minuto. Queste metriche includono il numero di [eventi](#) abbinati da una [regola](#) e il numero di volte in cui una [destinazione](#) viene richiamata da una regola. Quando una regola viene eseguita in EventBridge, vengono richiamati tutte le destinazioni associate alla regola. È possibile monitorare il comportamento di EventBridge tramite CloudWatch nei seguenti modi.

- Puoi monitorare le [metriche EventBridge](#) disponibili per le regole EventBridge dal pannello di controllo di CloudWatch. Puoi quindi utilizzare le funzionalità di CloudWatch, come gli allarmi CloudWatch, per impostare allarmi per determinate metriche. Se tali metriche raggiungono i valori di soglia personalizzati specificati negli allarmi, riceverai notifiche e potrai agire di conseguenza.
- Puoi impostare File di log Amazon CloudWatch come destinazione della regola EventBridge. EventBridge crea quindi flussi di log e File di log Amazon CloudWatch memorizza il testo degli eventi come voci di log. Per ulteriori informazioni, consulta l'argomento relativo a [EventBridge e File di log Amazon CloudWatch](#).

Per ulteriori informazioni sul debug della consegna e sull'archiviazione degli eventi EventBridge, consulta i seguenti argomenti:

- [Policy di ripetizione degli eventi e utilizzo delle code DLQ](#)
- [Archiviazione degli eventi EventBridge](#)

Condivisione di S3 on Outposts tramite AWS RAM

Amazon S3 on Outposts supporta la condivisione della capacità S3 su più account all'interno di un'organizzazione utilizzando AWS Resource Access Manager ([AWS RAM](#)). Con la condivisione di S3 on Outposts, puoi consentire ad altri di creare e gestire bucket, endpoint e punti di accesso sul tuo Outpost.

In questo argomento viene illustrato come utilizzare AWS RAM per condividere S3 on Outposts e le risorse correlate con un altro Account AWS nella tua organizzazione AWS.

Prerequisiti

- L'account proprietario dell'Outpost ha un'organizzazione configurata in AWS Organizations. Per ulteriori informazioni sulla configurazione di un'organizzazione, consulta [Creazione di un'organizzazione](#) nella Guida per l'utente di AWS Organizations.
- L'organizzazione include Account AWS con cui vuoi condividere la tua capacità di S3 su Outposts. Per ulteriori informazioni, consulta la sezione [Invio degli inviti agli Account AWS](#) nella Guida per l'utente di AWS Organizations.
- Seleziona una delle seguenti opzioni per la condivisione. La seconda risorsa (Sottoreti o Outpost) deve essere selezionata in modo che siano accessibili anche gli endpoint. Gli endpoint sono un requisito di rete per accedere ai dati archiviati in S3 on Outposts.

Opzione 1	Opzione 2
S3 on Outposts	S3 on Outposts
Consente all'utente di creare bucket sugli Outpost e sui punti di accesso e di aggiungere oggetti a tali bucket.	Consente all'utente di creare bucket sugli Outpost e sui punti di accesso e di aggiungere oggetti a tali bucket.
Sottoreti	Outposts
Consente all'utente di utilizzare il cloud privato virtuale (VPC) e gli endpoint associati alla sottorete.	Consente all'utente di visualizzare i grafici di capacità S3 e la pagina iniziale della console AWS Outposts. Consente inoltre agli utenti di creare sottoreti su Outpost condivisi e di creare endpoint.

Procedura

1. Esegui l'accesso a Console di gestione AWS utilizzando Account AWS, il proprietario dell'Outpost, quindi apri la console AWS RAM all'indirizzo <https://console.aws.amazon.com/ram/home>.
2. Verifica di aver abilitato la condivisione con AWS Organizations in AWS RAM. Per informazioni, consulta la sezione [Abilitazione della condivisione con AWS Organizations](#) nella Guida per l'utente di AWS RAM.
3. Utilizzare l'opzione 1 o l'opzione 2 nei [prerequisiti](#) per creare una condivisione di risorse. Se hai diverse risorse S3 su Outposts, seleziona gli Amazon Resource Name (ARN) delle risorse che desideri condividere. Per abilitare gli endpoint, condividi la sottorete o l'Outpost.

Per ulteriori informazioni sulla creazione di una condivisione di risorse, consulta la sezione [Creazione di una condivisione di risorse](#) nella Guida per l'utente di AWS RAM.

4. L'Account AWS con cui hai condiviso le tue risorse dovrebbe ora utilizzare S3 on Outposts. A seconda dell'opzione selezionata nei [prerequisiti](#), fornisci le seguenti informazioni all'utente dell'account:

Opzione 1	Opzione 2
L'ID dell'Outpost	L'ID dell'Outpost
L'ID del VPC	
L'ID sottorete	
L'ID del gruppo di sicurezza	

Note

L'utente può confermare che le risorse sono state condivise con lui utilizzando la console AWS RAM, la console AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. L'utente può visualizzare le condivisioni di risorse esistenti utilizzando il comando della CLI [get-resource shares](#).

Esempi di utilizzo

Dopo aver condiviso le risorse S3 on Outposts con un altro account, tale account può gestire bucket e oggetti sul tuo Outpost. Se hai condiviso la risorsa Subnets (Sottoreti), tale account può utilizzare l'endpoint creato. Negli esempi seguenti viene illustrato come un utente può impiegare la AWS CLI per interagire con il tuo Outpost dopo aver condiviso queste risorse.

Example : creazione di un bucket

Nell'esempio seguente viene creato un bucket denominato *amzn-s3-demo-bucket1* sull'Outpost *op-01ac5d28a6a232904*. Prima di utilizzare questo comando, sostituisci ciascun *user input placeholder* con i valori appropriati per il tuo caso d'uso.

```
aws s3control create-bucket --bucket amzn-s3-demo-bucket1 --outpost-id op-01ac5d28a6a232904
```

Per ulteriori informazioni su questo comando, consulta [create-bucket](#) nella Guida di riferimento AWS CLI.

Example : creazione di un punto di accesso

Nell'esempio seguente viene creato un punto di accesso su un Outpost utilizzando i parametri di esempio nella tabella seguente. Prima di utilizzare questo comando, sostituisci i valori *user input placeholder* e il codice Regione AWS con i valori appropriati per il tuo caso d'uso.

Parametro	Valore
ID account	<i>111122223333</i>
Nome del punto di accesso	<i>example-outpost-access-point</i>
ID Outpost	<i>op-01ac5d28a6a232904</i>
Nome del bucket dell'Outpost	<i>amzn-s3-demo-bucket1</i>
ID VPC	<i>vpc-1a2b3c4d5e6f7g8h9</i>

Note

Il parametro ID account deve essere l'ID Account AWS del proprietario del bucket, ossia l'utente condiviso.

```
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
```

Per ulteriori informazioni su questo comando, consulta [create-access-point](#) nella Guida di riferimento di AWS CLI.

Example : caricamento di un oggetto

Nell'esempio seguente viene caricato il file **my_image.jpg** dal file system locale dell'utente in un oggetto denominato **images/my_image.jpg** tramite il punto di accesso **example-outpost-access-point** sull'Outpost **op-01ac5d28a6a232904**, di proprietà dell'account AWS **111122223333**. Prima di utilizzare questo comando, sostituisci i valori **user input placeholder** e il codice Regione AWS con i valori appropriati per il tuo caso d'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
```

Per ulteriori informazioni, su questo comando, consulta [put-object](#) nella Guida di riferimento di AWS CLI.

Note

Se questa operazione si traduce in un errore Resource not found (Risorsa non trovata) o non risponde, il tuo VPC potrebbe non disporre di un endpoint condiviso.

Per verificare se esiste un endpoint condiviso, utilizza il comando AWS CLI [list-shared-endpoints](#). Se non esiste un endpoint condiviso, collabora con il proprietario di Outpost per crearne uno. Per ulteriori informazioni, consulta l'argomento relativo all'operazione

[ListSharedEndpoints](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Example : creazione di un endpoint

Nell'esempio seguente viene creato un endpoint per un Outpost condiviso. Prima di utilizzare questo comando, sostituisci i valori *user input placeholder* per l'ID dell'Outpost, l'ID della sottorete e l'ID del gruppo di sicurezza con i valori appropriati per il tuo caso d'uso.

Note

L'utente può eseguire questa operazione solo se la condivisione di risorse include la risorsa Outposts.

```
aws s3outposts create-endpoint --outposts-id op-01ac5d28a6a232904 --subnet-id XXXXXX --  
security-group-id XXXXXX
```

Per ulteriori informazioni su questo comando, consultare [create-endpoint](#) nella Guida di riferimento di AWS CLI.

Altri Servizi AWS che utilizzano S3 su Outposts

Gli altri Servizi AWS che vengono eseguiti localmente in AWS Outposts possono anche utilizzare la capacità di Amazon S3 su Outposts. In Amazon CloudWatch lo spazio dei nomi S3Outposts mostra i parametri dettagliati dei bucket in S3 su Outposts che tuttavia non includono l'utilizzo per altri Servizi AWS. Per gestire la capacità di S3 su Outposts che viene utilizzata da altri Servizi AWS, consulta le informazioni nella tabella seguente.

Servizio AWS	Descrizione	Ulteriori informazioni
Amazon S3	Tutto l'utilizzo diretto di S3 on Outposts ha un parametro CloudWatch di bucket e account corrispondente.	Vedi i parametri

Servizio AWS	Descrizione	Ulteriori informazioni
Amazon Elastic Block Store (Amazon EBS)	Per Amazon EBS su Outposts, puoi scegliere un AWS Outpost come destinazione snapshot e archiviare localmente nel tuo S3 su Outpost.	Ulteriori informazioni
Amazon Relational Database Service (Amazon RDS)	Puoi utilizzare i backup locali di Amazon RDS per archiviare i backup RDS localmente sul tuo Outpost.	Ulteriori informazioni

Monitoraggio di S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [. Che cos'è Amazon S3 su Outposts?](#)

Per ulteriori informazioni su come monitorare la capacità di archiviazione di Amazon S3 su Outposts, consulta i seguenti argomenti.

Argomenti

- [Gestione della capacità di S3 su Outposts con parametri Amazon CloudWatch](#)
- [Ricezione di notifiche di eventi S3 su Outposts utilizzando Eventi Amazon CloudWatch](#)
- [Monitoraggio di S3 su Outposts con i log AWS CloudTrail](#)

Gestione della capacità di S3 su Outposts con parametri Amazon CloudWatch

A supporto della gestione della capacità S3 fissa su Outposts, ti consigliamo di creare avvisi CloudWatch che informano quando l'utilizzo dello spazio di archiviazione supera una determinata soglia. Per ulteriori informazioni sui parametri CloudWatch per S3 su Outposts, consulta [Metriche CloudWatch](#). Se non c'è spazio sufficiente per archiviare un oggetto nell'outpost, l'API restituirà una ICE, ovvero una esenzione da capacità insufficiente. Per liberare spazio, puoi creare allarmi CloudWatch che attivano l'eliminazione esplicita dei dati o utilizzare una policy di scadenza del ciclo di vita per far scadere gli oggetti. Per salvare i dati prima dell'eliminazione, puoi utilizzare AWS DataSync per copiare i dati dal tuo bucket Amazon S3 su Outposts a un bucket S3 in una Regione AWS. Per ulteriori informazioni sull'utilizzo di DataSync, consulta [Nozioni di base di AWS DataSync](#) nella Guida per l'utente di AWS DataSync.

Metriche CloudWatch

Lo spazio dei nomi S3Outposts include i seguenti parametri per i bucket Amazon S3 on Outposts. È possibile monitorare il numero totale di byte S3 on Outposts di cui è stato eseguito il provisioning, il totale dei byte liberi disponibili per gli oggetti e la dimensione totale di tutti gli oggetti per un determinato bucket. Esistono parametri relativi a bucket o account per tutti gli usi diretti di S3. L'utilizzo indiretto di S3, ad esempio l'archiviazione di snapshot locali di Amazon Elastic Block Store o dei backup di Amazon Relational Database Service su Outposts, consuma la capacità di S3, ma non è incluso nei parametri relativi a bucket o account. Per ulteriori informazioni sugli snapshot locali di Amazon EBS, consulta [Snapshot locali di Amazon EBS su Outposts](#). Per visualizzare il report sui costi di Amazon EBS, visita <https://console.aws.amazon.com/costmanagement/>.

Note

S3 su Outposts supporta solo i parametri riportati di seguito e non supporta altri parametri Amazon S3.

Poiché S3 su Outposts ha una capacità fissa limitata, si consiglia di creare avvisi CloudWatch che informano quando l'utilizzo dello spazio di archiviazione supera una determinata soglia.

Parametro	Descrizione	Periodo di tempo	Unità	Tipo
OutpostTotalBytes	La capacità totale di cui è stato eseguito il provisioning in byte per un outpost.	5 minuti	Byte	S3 on Outposts
OutpostFreeBytes	Il numero di byte gratuiti disponibili in un Outpost per archiviare i dati dei clienti.	5 minuti	Byte	S3 on Outposts
BucketUsedBytes	La dimensione totale di tutti gli oggetti per il bucket specificato.	5 minuti	Byte	S3 su Outposts. Solo utilizzo diretto di S3.

Parametro	Descrizione	Periodo di tempo	Unità	Tipo
AccountTotalBytes	La dimensione totale di tutti gli oggetti per l'account Outposts specificato.	5 minuti	Byte	S3 su Outposts. Solo utilizzo diretto di S3.
BytesPendingReplication	Numero totale di byte di oggetti in attesa di replica per una determinata regola di replica. Per ulteriori informazioni su come abilitare le metriche di replica, consulta l'argomento relativo alla creazione di regole di replica tra outpost .	5 minuti	Byte	Facoltativo. Per Replica Amazon S3 su Outposts.
OperationsPendingReplication	Numero totale di operazioni in attesa di replica per una determinata regola di replica. Per ulteriori informazioni su come abilitare le metriche di replica, consulta l'argomento relativo alla creazione di regole di replica tra outpost .	5 minuti	Conteggi	Facoltativo. Per Replica Amazon S3 su Outposts.

Parametro	Descrizione	Periodo di tempo	Unità	Tipo
ReplicaLatency	Numero corrente di secondi entro i quali i bucket di destinazione della replica sono in ritardo rispetto al bucket di origine per una determinata regola di replica. Per ulteriori informazioni su come abilitare le metriche di replica, consulta l'argomento relativo alla creazione di regole di replica tra outpost .	5 minuti	Secondi	Facoltativo. Per Replica Amazon S3 su Outposts.

Ricezione di notifiche di eventi S3 su Outposts utilizzando Eventi Amazon CloudWatch

Puoi usare Eventi Amazon CloudWatch per creare una regola per ogni evento API di Amazon S3 su Outposts. Quando crei una regola, puoi scegliere di ricevere notifiche da tutte le destinazioni supportate di CloudWatch, tra cui Amazon Simple Queue Service (Amazon SQS), Servizio di notifica semplice Amazon (Amazon SNS) e AWS Lambda. Per ulteriori informazioni, consulta l'elenco dei [servizi AWS che possono essere destinazioni per Eventi CloudWatch](#) nella Guida per l'utente di Eventi Amazon CloudWatch. Per scegliere un servizio di destinazione da utilizzare con S3 su Outposts, consulta [Creazione di una regola di CloudWatch Events che si attiva su una chiamata API AWS utilizzando AWS CloudTrail](#) nella Guida per l'utente di Eventi Amazon CloudWatch.

Note

Per le operazioni di oggetti S3 su Outposts, gli eventi di chiamata API AWS inviati da CloudTrail corrisponderanno alle tue regole solo se i trail (facoltativamente con i selettori di eventi) sono configurati per ricevere tali eventi. Per ulteriori informazioni, consulta [Utilizzo dei file di log di CloudTrail](#) nella Guida per l'utente di AWS CloudTrail.

Example

Di seguito è riportata una regola di esempio per l'operazione `DeleteObject`. Per utilizzare questa regola di esempio, sostituisci `amzn-s3-demo-bucket1` con il nome del bucket S3 su 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"  
      ]  
    }  
  }  
}
```

Monitoraggio di S3 su Outposts con i log AWS CloudTrail

Amazon S3 su Outposts è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un Servizio AWS in Amazon S3 su Outposts. Puoi utilizzare AWS CloudTrail per ottenere informazioni relative alle richieste S3 su Outposts a livello di bucket e a livello di oggetto per controllare e registrare l'attività degli eventi di S3 su Outposts.

Per abilitare gli eventi di dati CloudTrail per tutti i bucket Outposts o per un elenco di bucket Outposts specifici, è necessario [creare un trail manualmente in CloudTrail](#). Per ulteriori informazioni sulle voci del file di log di CloudTrail, consulta le [voci del file di log di S3 su Outposts](#).

Per un elenco completo degli eventi di dati di CloudTrail per S3 su Outposts, consulta [Eventi di dati di Amazon S3 in CloudTrail](#) nella Guida per l'utente di Amazon S3.

Note

- È una best practice creare una policy del ciclo di vita per il bucket Outposts degli eventi di dati AWS CloudTrail. Configura la policy del ciclo di vita in modo tale da rimuovere periodicamente i file di log al termine del periodo di tempo desiderato per l'audit. In questo modo, si riduce la quantità di dati analizzati da Amazon Athena per ogni query. Per ulteriori informazioni, consulta [Creazione e gestione di una configurazione del ciclo di vita per un bucket Amazon S3 su Outposts](#).
- Per esempi su come eseguire query sui log CloudTrail, consulta il post del Blog sui Big Data di AWS dal titolo [Analisi dei problemi di sicurezza, conformità e attività operativa tramite AWS CloudTrail e Amazon Athena](#).

Abilitare la registrazione CloudTrail per gli oggetti in un bucket S3 su Outposts

Puoi utilizzare la console Amazon S3 per abilitare un trail AWS CloudTrail per registrare gli eventi di dati per gli oggetti in un bucket Amazon S3 su Outposts. CloudTrail supporta la registrazione delle operazioni API a livello di oggetto di S3 su Outposts, ad esempio GetObject, DeleteObject e PutObject. Questi eventi vengono chiamati eventi di dati.

Per impostazione predefinita, i trail di CloudTrail non registrano gli eventi di dati. È possibile tuttavia configurare i trail per registrare gli eventi di dati per i bucket S3 su Outposts specificati oppure per registrare gli eventi di dati per tutti i bucket S3 su Outposts nel proprio Account AWS.

CloudTrail non popola gli eventi dati nella cronologia eventi CloudTrail. Inoltre, non tutte le operazioni API a livello di bucket S3 su Outposts vengono popolate nella cronologia degli eventi CloudTrail. Per ulteriori informazioni su come eseguire query sui log CloudTrail, consulta l'articolo sull'[uso degli schemi di filtro File di log Amazon CloudWatch e di Amazon Athena per eseguire query sui log CloudTrail](#) in AWS Knowledge Center.

Per configurare un trail per registrare gli eventi di dati per un bucket S3 su Outposts, puoi utilizzare la console AWS CloudTrail o la console Amazon S3. Se stai configurando un trail per registrare gli eventi di dati per tutti i bucket S3 su Outposts nell'Account AWS, è più semplice utilizzare la console CloudTrail. Per informazioni sull'utilizzo della console CloudTrail per configurare un trail per registrare gli eventi di dati S3 su Outposts, consulta [Eventi di dati](#) nella Guida per l'utente di AWS CloudTrail.

⚠ Important

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di AWS CloudTrail](#).

La procedura seguente mostra come utilizzare la console Amazon S3 per abilitare un trail CloudTrail per registrare gli eventi di dati per un bucket S3 su Outposts.

ⓘ Note

L'Account AWS che crea il bucket ne è il proprietario ed è l'unico in grado di configurare gli eventi di dati S3 su Outposts da inviare a AWS CloudTrail.

Per abilitare la registrazione degli eventi di dati CloudTrail per gli oggetti in un bucket S3 su Outposts

1. Accedere a Console di gestione AWS e aprire la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, seleziona Outposts buckets (Bucket Outposts).
3. Seleziona il nome del bucket Outposts di cui desideri registrare gli eventi di dati utilizzando CloudTrail.
4. Scegli Properties (Proprietà).
5. Nella sezione Eventi di dati AWS CloudTrail, scegli Configura in CloudTrail.

Si apre la console AWS CloudTrail.

Puoi creare un nuovo trail CloudTrail o riutilizzare un trail esistente e configurare la registrazione degli eventi di dati di S3 su Outposts nel tuo trail.

6. Nella pagina Pannello di controllo della console CloudTrail, scegli Crea trail.
7. Nella pagina Fase 1 - Seleziona attributi trail, specifica un nome per il percorso, scegli un bucket S3 per archiviare i log del trail, specifica le altre impostazioni desiderate e quindi scegli Avanti.
8. Nella pagina Fase 2 - Seleziona eventi di log, in Tipo di evento, scegli Eventi di dati.

In Tipo di evento di dati, scegli S3 Outposts. Scegli Next (Successivo).

Note

- Quando crei un trail e configuri la registrazione degli eventi di dati per S3 su Outposts, devi specificare correttamente il tipo di evento di dati.
- Se utilizzi la console CloudTrail, scegli S3 Outposts in Tipo di evento di dati. Per informazioni su come creare percorsi nella console CloudTrail, consulta [Creazione e aggiornamento di un trail nella console](#) nella Guida per l'utente di AWS CloudTrail. Per informazioni su come configurare la registrazione degli eventi di dati di S3 su Outposts nella console CloudTrail, consulta [Registrazione di eventi di dati per oggetti Amazon S3](#) nella Guida per l'utente di AWS CloudTrail.
- Se usi la AWS Command Line Interface (AWS CLI) o gli SDK AWS, imposta il campo `resources.type` su `AWS::S3Outposts::Object`. Per ulteriori informazioni su come registrare gli eventi di dati di S3 su Outposts con la AWS CLI, consulta [Registrazione di eventi Amazon S3](#) nella Guida per l'utente di AWS CloudTrail.
- Se utilizzi la console CloudTrail o la console Amazon S3 per configurare un trail per registrare gli eventi di dati per un bucket S3 su Outposts, la console Amazon S3 mostra che la registrazione a livello di oggetti è abilitata per il bucket.

9. Nella pagina Fase 3 - Verifica e crea, rivedi gli attributi del trail e i log eventi che hai configurato. Quindi scegli Crea trail.

Per disabilitare la registrazione degli eventi di dati CloudTrail per gli oggetti in un bucket S3 su Outposts

1. Accedi alla Console di gestione AWS e apri la console CloudTrail all'indirizzo <https://console.aws.amazon.com/cloudtrail/>.
2. Nel pannello di navigazione a sinistra, scegli Trail.
3. Scegli il nome del trail che hai creato per registrare i log eventi del bucket S3 su Outposts.
4. Nella pagina dei dettagli del trail, scegli Interrompi la registrazione nell'angolo in alto a destra.
5. Nella finestra di dialogo visualizzata, scegli Interrompi la registrazione.

Voci del file di log di AWS CloudTrail di Amazon S3 su Outposts

Gli eventi di gestione di Amazon S3 su Outposts sono disponibili tramite AWS CloudTrail. Inoltre, facoltativamente, puoi [abilitare la registrazione per gli eventi di dati in AWS CloudTrail](#).

Un trail è una configurazione che consente il recapito di eventi come i file di log in un bucket S3 in una regione che specifichi. I log CloudTrail per i bucket Outposts includono un nuovo campo, `edgeDeviceDetails`, che identifica l'Outpost in cui si trova il bucket specificato.

I campi di log aggiuntivi includono l'operazione richiesta, la data e l'ora dell'operazione nonché i parametri della richiesta. I file di log CloudTrail non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di log CloudTrail che illustra un'operazione [PutObject](#) su 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",  

```

```
"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": "29xXQBV20
+x0HKItvzY1suLv1i6A52E0z0X159fpfsItYd58JhXwKxXAXI4IQkp6",
    "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"
}
```

Sviluppo con Amazon S3 su Outposts

Con Amazon S3 su Outposts è possibile creare bucket S3 su AWS Outposts, nonché archiviare e recuperare facilmente gli oggetti on-Premise per le applicazioni che richiedono l'accesso ai dati in locale, l'elaborazione dei dati in locale e la residenza dei dati. S3 su Outposts fornisce una nuova classe di archiviazione, S3 Outposts (OUTPOSTS), che utilizza le API Amazon S3 ed è progettata per archiviare i dati in modo durevole e ridondante su più dispositivi e server su AWS Outposts. Comunichi con il bucket Outpost utilizzando un punto di accesso e una connessione di endpoint su un Virtual Private Cloud (VPC). Sui bucket Outposts puoi utilizzare le stesse API e caratteristiche di Amazon S3, comprese policy di accesso, crittografia e tagging. Puoi utilizzare S3 su Outposts tramite la Console di gestione AWS, AWS Command Line Interface (AWS CLI), gli SDK AWS o l'API REST. Per ulteriori informazioni, consulta [Che cos'è Amazon S3 su Outposts?](#)

I seguenti argomenti forniscono informazioni sullo sviluppo con S3 su Outposts

Argomenti

- [Regioni in cui è supportato S3 su Outposts](#)
- [Operazioni API in Amazon S3 su Outposts](#)
- [Configurazione del client di controllo S3 per S3 su Outposts utilizzando SDK per Java](#)
- [Esecuzione di richieste a S3 su Outposts su IPv6](#)

Regioni in cui è supportato S3 su Outposts

S3 su Outposts è supportato nelle Regioni AWS seguenti.

- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Stati Uniti orientali (Ohio) (us-east-2)
- Stati Uniti occidentali (California settentrionale) (us-west-1)
- Stati Uniti occidentali (Oregon) (us-west-2)
- Africa (Città del Capo) (af-south-1)
- Asia Pacifico (Giacarta) (ap-southeast-3)
- Asia Pacifico (Mumbai) (ap-south-1)
- Asia Pacifico (Osaka-Locale) (ap-northeast-3)
- Asia Pacifico (Seoul) (ap-northeast-2)

- Asia Pacifico (Singapore) (ap-southeast-1)
- Asia Pacifico (Sydney) (ap-southeast-2)
- Asia Pacifico (Tokyo) (ap-northeast-1)
- Canada (Centrale) (ca-central-1)
- Europa (Francoforte) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londra) (eu-west-2)
- Europa (Milano) (eu-south-1)
- Europa (Parigi) (eu-west-3)
- Europa (Stoccolma) (eu-north-1)
- Israele (Tel Aviv) (il-central-1)
- Medio Oriente (Bahrein) (me-south-1)
- Sud America (San Paolo) (sa-east-1)
- AWS GovCloud (Stati Uniti-Est) (us-gov-east-1)
- AWS GovCloud (Stati Uniti-Ovest) (us-gov-west-1)

Operazioni API in Amazon S3 su Outposts

In questo argomento viene fornito l'elenco delle operazioni API su Amazon S3, Amazon S3 Control e Amazon S3 su Outposts che puoi utilizzare in Amazon S3 su Outposts.

Argomenti

- [Operazioni API Amazon S3 per la gestione degli oggetti](#)
- [Operazioni API Amazon S3 Control per la gestione dei bucket](#)
- [Operazioni API S3 su Outposts per la gestione di Outposts](#)

Operazioni API Amazon S3 per la gestione degli oggetti

S3 su Outposts è progettato per utilizzare le stesse operazioni API sugli oggetti di Amazon S3.

È necessario utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outpost.

Quando utilizzi un'operazione API di oggetti con S3 su Outposts, fornisci il nome della risorsa Amazon (ARN) del punto di accesso Outposts o l'alias del punto di accesso. Per ulteriori informazioni

sugli alias del punto di accesso, consulta [Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts](#).

Amazon S3 su Outposts supporta le seguenti operazioni API Amazon S3:

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [DeleteObjectTagging](#)
- [GetObject](#)
- [GetObjectTagging](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListMultipartUploads](#)
- [ListObjects](#)
- [ListObjectsV2](#)
- [ListObjectVersions](#)
- [ListParts](#)
- [PutObject](#)
- [PutObjectTagging](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Operazioni API Amazon S3 Control per la gestione dei bucket

S3 su Outposts supporta le seguenti operazioni API Amazon S3 Control per le operazioni sui bucket.

- [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](#)

Operazioni API S3 su Outposts per la gestione di Outposts

S3 su Outposts supporta le seguenti operazioni API Amazon S3 su Outposts per la gestione degli endpoint.

- [CreateEndpoint](#)
- [DeleteEndpoint](#)
- [ListEndpoints](#)

- [ListOutpostsWithS3](#)
- [ListSharedEndpoints](#)

Configurazione del client di controllo S3 per S3 su Outposts utilizzando SDK per Java

Nell'esempio seguente viene configurato il client di controllo Amazon S3 per Amazon S3 su Outposts mediante AWS SDK per Java. Per utilizzare questo comando, sostituisci *user input placeholder* con le tue informazioni.

```
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();

}
```

Esecuzione di richieste a S3 su Outposts su IPv6

Gli endpoint dual-stack Amazon S3 su Outposts e S3 su Outposts supportano le richieste ai bucket S3 su Outposts utilizzando il protocollo IPv6 o IPv4. Con il supporto IPv6 per S3 su Outposts, è possibile accedere e gestire i bucket e le risorse del piano di controllo (control-plane) tramite le API S3 su Outposts su reti IPv6.

Note

Le [operazioni su oggetti di S3 su Outposts](#) (come PutObject o GetObject) non sono supportate sulle reti IPv6.

Non sono previsti costi aggiuntivi per l'accesso a S3 su Outposts su reti IPv6. Per ulteriori informazioni su S3 su Outposts, vedere [Prezzi di S3 su Outposts](#).

Argomenti

- [Nozioni di base su IPv6](#)
- [Utilizzo di endpoint dual-stack per effettuare richieste su una rete IPv6](#)
- [Utilizzo degli indirizzi IPv6 nelle policy IAM](#)
- [Test di compatibilità degli indirizzi IP](#)
- [Utilizzo di IPv6 con AWS PrivateLink](#)
- [Utilizzo degli endpoint dual-stack S3 su Outposts](#)

Nozioni di base su IPv6

Per effettuare una richiesta a un bucket S3 su Outposts su IPv6, è necessario utilizzare un endpoint dual-stack. Nella sezione seguente viene descritto come effettuare richieste su IPv6 utilizzando gli endpoint dual-stack.

Di seguito sono descritti alcuni punti da prendere in considerazione prima di provare ad accedere a un bucket S3 su Outposts su IPv6:

- Il client e la rete che eseguono l'accesso al bucket devono essere abilitati a utilizzare IPv6.
- Per l'accesso a IPv6 sono supportate sia le richieste in stile percorso sia quelle in stile hosting virtuale. Per ulteriori informazioni, consulta [Utilizzo degli endpoint dual-stack S3 su Outposts](#).
- Se si utilizza il filtro degli indirizzi IP di origine nelle policy dell'utente AWS Identity and Access Management (IAM) o del bucket S3 su Outposts, è necessario aggiornare le policy in modo da includere gli intervalli di indirizzi IPv6.

Note

Questo requisito si applica solo alle operazioni dei bucket S3 su Outposts e alle risorse del piano di controllo (control-plane) su reti IPv6. Le [operazioni su oggetti di S3 su Outposts](#) non sono supportate sulle reti IPv6.

- Quando si utilizza IPv6, i file di log degli accessi al server generano indirizzi IP in un formato IPv6. È necessario aggiornare il software, gli script e gli strumenti esistenti utilizzati per analizzare i file di log di S3 su Outposts affinché possano analizzare gli indirizzi IP remoti in formato IPv6. Il software,

gli script e gli strumenti aggiornati analizzeranno quindi correttamente gli indirizzi IP remoti in formato IPv6.

Utilizzo di endpoint dual-stack per effettuare richieste su una rete IPv6

Per effettuare richieste con chiamate API di S3 su Outposts su IPv6, è possibile utilizzare gli endpoint dual-stack tramite AWS CLI o AWS SDK. Le [operazioni API di controllo Amazon S3](#) e le [operazioni API S3 su Outposts](#) funzionano allo stesso modo indipendentemente dal fatto che si acceda a S3 su Outposts tramite un protocollo IPv6 o un protocollo IPv4. Tuttavia, occorre tenere presente che le [operazioni su oggetti di S3 su Outposts](#) (come PutObject o GetObject) non sono supportate sulle reti IPv6.

Quando si utilizzano AWS Command Line Interface (AWS CLI) e gli SDK AWS, è possibile servirsi di un parametro o flag per passare a un endpoint dual-stack. È inoltre possibile specificare l'endpoint dual-stack direttamente come sostituzione dell'endpoint S3 su Outposts nel file di configurazione.

È possibile utilizzare un endpoint dual-stack per accedere a un bucket S3 su Outposts su IPv6 da uno qualsiasi dei seguenti elementi:

- La AWS CLI, consulta [Utilizzo degli endpoint dual-stack dall'AWS CLI](#).
- Gli SDK AWS, consulta [Utilizzo degli endpoint dual-stack S3 su Outposts dagli SDK AWS](#).

Utilizzo degli indirizzi IPv6 nelle policy IAM

Prima di tentare di accedere a un bucket S3 su Outposts tramite un protocollo IPv6, assicurarsi che le policy degli utenti IAM o del bucket S3 su Outposts utilizzate per il filtro degli indirizzi IP siano aggiornate per includere gli intervalli di indirizzi IPv6. Se le policy di filtro degli indirizzi IP non vengono aggiornate per gestire gli indirizzi IPv6, è possibile perdere l'accesso a un bucket S3 su Outposts mentre si prova a utilizzare il protocollo IPv6.

Le policy IAM che filtrano gli indirizzi IP utilizzano gli [operatori di condizione degli indirizzi IP](#). La seguente policy del bucket S3 su Outposts identifica l'intervallo IP 54.240.143.* degli indirizzi IPv4 consentiti tramite gli operatori di condizione degli indirizzi IP. A qualsiasi indirizzo IP non incluso in questo intervallo verrà negato l'accesso al bucket S3 su Outposts (DOC-EXAMPLE-BUCKET). Poiché tutti gli indirizzi IPv6 non sono inclusi nell'intervallo consentito, questa policy impedisce agli indirizzi IPv6 di accedere a 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"
        }
      }
    }
  ]
}
```

È possibile modificare l'elemento `Condition` della policy del bucket S3 su Outposts per consentire entrambi gli intervalli di indirizzi IPv4 (54.240.143.0/24) e IPv6 (2001:DB8:1234:5678::/64), come mostrato nell'esempio che segue. È possibile utilizzare lo stesso tipo di blocco `Condition` mostrato nell'esempio per aggiornare sia le policy del bucket sia le policy utente IAM.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": [
      "54.240.143.0/24",
      "2001:DB8:1234:5678::/64"
    ]
  }
}
```

Prima di utilizzare IPv6, è necessario aggiornare tutte le policy del bucket e utente IAM pertinenti che utilizzano il filtro degli indirizzi IP per consentire gli intervalli di indirizzi IPv6. Ti consigliamo di aggiornare le policy IAM con gli intervalli di indirizzi IPv6 dell'organizzazione oltre agli intervalli di indirizzi IPv4 esistenti. Per un esempio di una policy del bucket che consenta l'accesso sia su IPv6 sia su IPv4, consulta [Limitare l'accesso a indirizzi IP specifici](#).

È possibile esaminare le policy utente IAM tramite la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>. Per ulteriori informazioni su IAM, consulta la [Guida per l'utente di IAM](#). Per informazioni sulla modifica delle policy dei bucket S3 su Outposts, consulta [Aggiunta o modifica di una policy di un bucket Amazon S3 su Outposts](#).

Test di compatibilità degli indirizzi IP

Se si utilizza un'istanza Linux o Unix o una piattaforma macOS X, è possibile testare l'accesso a un endpoint dual-stack su IPv6. Ad esempio, per testare la connessione agli endpoint Amazon S3 su Outposts su IPv6, usare il comando dig:

```
dig s3-outposts.us-west-2.api.aws AAAA +short
```

Se l'endpoint dual-stack su una rete IPv6 è configurato correttamente, il comando dig restituisce gli indirizzi IPv6 connessi. Ad esempio:

```
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
```

Utilizzo di IPv6 con AWS PrivateLink

S3 su Outposts supporta il protocollo IPv6 per i servizi e gli endpoint di AWS PrivateLink. Con il supporto di AWS PrivateLink per il protocollo IPv6, è possibile connetterti agli endpoint del servizio all'interno del VPC su reti IPv6 sia da connessioni on-premises che da altre connessioni private. Il supporto IPv6 per [AWS PrivateLink per S3 su Outposts](#) consente inoltre di integrare AWS PrivateLink con endpoint dual-stack. Per istruzioni su come abilitare IPv6 per AWS PrivateLink, consulta [Accelerare l'adozione di IPv6 con servizi ed endpoint di AWS PrivateLink](#).

Note

Per aggiornare il tipo di indirizzo IP supportato da IPv4 a IPv6, consulta [Modificare il tipo di indirizzo IP supportato](#) nella Guida per l'utente di AWS PrivateLink.

Utilizzo di IPv6 con AWS PrivateLink

Se si utilizza AWS PrivateLink con IPv6, è necessario creare un endpoint di interfaccia IPv6 o VPC dual-stack. Per le istruzioni generali su come creare un endpoint VPC utilizzando la Console di gestione AWS, consulta [Accedere a un servizio AWS utilizzando un endpoint VPC di interfaccia](#) nella Guida per l'utente di AWS PrivateLink.

Console di gestione AWS

Utilizzare la procedura seguente per creare un endpoint VPC di interfaccia in grado di connettersi a S3 su Outposts.

1. Accedi alla Console di gestione AWS e apri la console VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Service category (Categoria servizio), scegli AWS services.
5. Per Nome servizio, scegli il servizio S3 su Outposts (com.amazonaws.us-east-1.s3-outposts).
6. Per VPC, scegli il VPC da cui si accederà a S3 su Outposts.
7. Per Sottoreti, scegli una sottorete per ogni zona di disponibilità dalla quale si accederà a S3 su Outposts. Non è possibile selezionare più sottoreti dalla stessa zona di disponibilità. Per ogni sottorete selezionata, viene creata una nuova interfaccia di rete dell'endpoint. Per impostazione predefinita, alle interfacce di rete dell'endpoint vengono assegnati gli indirizzi IP degli intervalli di indirizzi IP della sottorete. Per designare un indirizzo IP per un'interfaccia di rete dell'endpoint, scegli Designazione di indirizzi IP e inserisci un indirizzo IPv6 dall'intervallo di indirizzi di sottorete.
8. Per Tipo di indirizzo IP, scegli Dualstack. Assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6.
9. Per Gruppi di sicurezza, scegli i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint per l'endpoint VPC. Per impostazione predefinita, il gruppo di sicurezza predefinito viene associato al VPC.
10. Per Policy, scegli Accesso completo per consentire a tutti i principali di eseguire tutte le operazioni su tutte le risorse dell'endpoint VPC. Altrimenti, scegli Personalizzato, per allegare una policy dell'endpoint VPC che controlla le autorizzazioni che i principali hanno per eseguire azioni sulle risorse attraverso l'endpoint. Questa opzione è disponibile solo se il

servizio supporta le policy dell'endpoint VPC. Per ulteriori informazioni, consulta [Policy di endpoint](#).

11. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
12. Seleziona Crea endpoint.

Example - Policy di bucket S3 su Outposts

Per consentire a S3 su Outposts di interagire con gli endpoint VPC, è possibile aggiornare la policy S3 su Outposts in questo modo:

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "s3-outposts:*",  
      "Resource": "*",  
      "Principal": "*"  
    }  
  ]  
}
```

AWS CLI

Note

Per abilitare la rete IPv6 sull'endpoint VPC, è necessario impostare IPv6 per il filtro SupportedIpAddressType per S3 su Outposts.

L'esempio seguente utilizza il comando `create-vpc-endpoint` per creare un nuovo endpoint di interfaccia dual-stack.

```
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"
```

A seconda della configurazione del servizio AWS PrivateLink, le connessioni endpoint appena create potrebbero dover essere accettate dal fornitore del servizio endpoint VPC prima di poter essere utilizzate. Per ulteriori informazioni, consulta [Accettare e rifiutare le richieste di connessione all'endpoint](#) nella Guida per l'utente di AWS PrivateLink.

L'esempio seguente utilizza il comando `modify-vpc-endpoint` per aggiornare l'endpoint VPC solo IPv in un endpoint dual-stack. L'endpoint dual-stack consente l'accesso a entrambe le reti 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"
```

Per ulteriori informazioni su come abilitare la rete IPv6 per AWS PrivateLink, consulta [Accelerare l'adozione di IPv6 con servizi ed endpoint di AWS PrivateLink](#).

Utilizzo degli endpoint dual-stack S3 su Outposts

Gli endpoint dual-stack S3 su Outposts supportano le richieste ai bucket S3 su Outposts su IPv6 e IPv4. In questa sezione viene descritto come utilizzare gli endpoint dual-stack S3 su Outposts.

Argomenti

- [Endpoint dual-stack S3 su Outposts](#)
- [Utilizzo degli endpoint dual-stack dall'AWS CLI](#)
- [Utilizzo degli endpoint dual-stack S3 su Outposts dagli SDK AWS](#)

Endpoint dual-stack S3 su Outposts

Quando si effettua una richiesta a un endpoint dual-stack, l'URL del bucket S3 su Outposts restituisce un indirizzo IPv6 o IPv4. Per ulteriori informazioni sull'accesso a un bucket S3 su Outposts su IPv6, consulta [Esecuzione di richieste a S3 su Outposts su IPv6](#).

Per accedere a un bucket S3 su Outposts tramite un endpoint dual-stack, usare un nome di endpoint in stile percorso. S3 su Outposts supporta solo i nomi di endpoint dual-stack regionali, il che significa che è necessario specificare la Regione come parte del nome.

Gli endpoint dual-stack FIPS in stile percorso usano la seguente convenzione di denominazione:

```
s3-outposts-fips.region.api.aws
```

Gli endpoint dual-stack non FIPS usano la seguente convenzione di denominazione:

```
s3-outposts.region.api.aws
```

 Note

I nomi degli endpoint in stile hosting virtuale non sono supportati in S3 su Outposts.

Utilizzo degli endpoint dual-stack dall'AWS CLI

In questa sezione vengono forniti esempi dei comandi dell'AWS CLI utilizzati per effettuare le richieste a un endpoint dual-stack. Per istruzioni sull'impostazione di AWS CLI, consulta [Nozioni di base tramite l'utilizzo di AWS CLI e SDK per Java](#).

Impostare il valore di configurazione `use_dualstack_endpoint` su `true` in un profilo nel file AWS Config per indirizzare tutte le richieste Amazon S3 effettuate dai comandi `s3` e `s3api` di AWS CLI all'endpoint dual-stack per la Regione specificata. La Regione va specificata nel file di configurazione o in un comando tramite l'opzione `--region`.

Quando si utilizzano gli endpoint dual-stack con AWS CLI, è supportato solo lo stile di indirizzamento `path`. Lo stile di indirizzamento, impostato nel file di configurazione, determina se il nome del bucket si trova nel nome host o nell'URL. Per ulteriori informazioni, consulta [s3outposts](#) nella AWS CLI Guida per l'utente.

Per utilizzare un endpoint dual-stack tramite AWS CLI, usare il parametro `--endpoint-url` con l'endpoint `http://s3.dualstack.region.amazonaws.com` o `https://s3-outposts-fips.region.api.aws` per qualsiasi comando `s3control` o `s3outposts`.

Ad esempio:

```
$ aws s3control list-regional-buckets --endpoint-url https://s3-outposts.region.api.aws
```

Utilizzo degli endpoint dual-stack S3 su Outposts dagli SDK AWS

In questa sezione vengono forniti esempi su come accedere all'endpoint dual-stack tramite gli SDK AWS.

AWS SDK for Java 2.x Esempio di endpoint Dual-Stack con

Negli esempi seguenti viene mostrato come usare le classi **S3ControlClient** e **S3OutpostsClient** per abilitare gli endpoint dual-stack durante la creazione di un client S3 su Outposts tramite AWS SDK for Java 2.x. Per istruzioni su come creare e testare un esempio Java funzionante per Amazon S3 su Outposts, consulta [Nozioni di base tramite l'utilizzo di AWS CLI e SDK per Java](#).

Example - Creare una classe **S3ControlClient** con gli endpoint dual-stack abilitati

```
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 - Creare una classe **S3OutpostsClient** con gli endpoint dual-stack abilitati

```
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 si utilizza AWS SDK for Java 2.x in Windows, potrebbe essere necessario impostare la seguente proprietà Java Virtual Machine (JVM):

```
java.net.preferIPv6Addresses=true
```