



Leitfaden

Amazon S3 in Outposts



API-Version 2006-03-01

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon S3 in Outposts: Leitfaden

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, Kunden irrezuführen oder Amazon in irgendeiner Weise herabzusetzen oder zu diskreditieren. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist S3 on Outposts?	1
Funktionsweise von S3 on Outposts	1
Regionen	2
Buckets	2
Objekte	3
Schlüssel	4
S3-Versioning	4
Versions-ID	4
Speicherklasse und Verschlüsselung	5
Bucket-Richtlinie	5
S3-on-Outposts-Zugriffspunkte	5
Funktionen von S3 on Outposts	6
Zugriffsverwaltung	6
Speicherprotokollierung und Überwachung	7
Starke Konsistenz	7
Zugehörige Services	7
Zugriff auf S3 on Outposts	8
AWS Management Console	8
AWS Command Line Interface	8
AWS SDKs	9
Bezahlung für S3 on Outposts	9
Nächste Schritte	9
Einrichten Ihres Outposts	11
Einen neuen -Outpost bestellen	11
Inwieweit S3 on Outposts anders ist	12
Technische Daten	12
Unterstützte Operationen API	13
Nicht unterstützte Amazon-S3-Funktionen	13
Netzwerkeinschränkungen	14
Erste Schritte mit S3 on Outposts	16
Verwenden der S3-Konsole	16
Einen Bucket, einen Zugriffspunkt und einen Endpunkt erstellen	17
Nächste Schritte	20
Verwenden von AWS CLI und SDK für Java	20

Schritt 1: Erstellen eines Buckets	21
Schritt 2: Erstellen eines Zugriffspunkts	22
Schritt 3: Erstellen eines Endpunkts	23
Schritt 4: Hochladen eines Objekts in einen S3-on-Outposts-Bucket	25
Vernetzung für S3 on Outposts	26
Auswählen des Netzwerkzugriffstyps	26
Zugriff auf Ihre S3-on-Outposts-Buckets und -Objekte	26
Verwalten von Verbindungen mit kontenübergreifenden Elastic Network-Schnittstellen	27
Arbeiten mit S3-on-Outposts-Buckets	28
Buckets	28
Zugriffspunkte	28
Endpunkte	29
APIOperationen auf S3 auf Outposts	29
Erstellen und Verwalten von S3 on Outposts-Buckets	31
Erstellen eines Buckets	31
Hinzufügen von Tags	35
Verwenden von Bucket-Richtlinien	37
Hinzufügen einer Bucket-Richtlinie	38
Anzeigen einer Bucket-Richtlinie	40
Löschen einer Bucket-Richtlinie	41
Beispiele für Bucket-Richtlinien	42
Auflisten von Buckets	46
Abrufen eines Buckets	48
Löschen des Buckets	49
Arbeiten mit Zugriffspunkten	51
Erstellen eines Zugriffspunkts	52
Verwenden eines Alias im Bucket-Stil für Ihren Zugriffspunkt.	54
Anzeigen einer Zugriffspunktconfiguration	58
Auflisten von Zugriffspunkten	59
Löschen eines Zugriffspunkts	60
Hinzufügen einer Zugriffspunktrichtlinie	61
Anzeigen einer Zugriffspunktrichtlinie	63
Arbeiten mit Endpunkten	64
Erstellen eines Endpunkts	66
Auflisten von Endpunkten	68
Löschen eines Endpunkts	69

Arbeiten mit S3-on-Outposts-Objekten	72
Hochladen eines Objekts	73
Kopieren eines Objekts	76
Verwendung des AWS SDK for Java	76
Ein Objekt abrufen	77
Auflisten von Objekten	81
Löschen von Objekten	84
Verwenden HeadBucket	88
Durchführen eines mehrteiligen Uploads	91
Durchführen eines mehrteiligen Uploads eines Objekts in einem S3-on-Outposts-Bucket	91
Kopieren eines großen Objekts in einem S3-on-Outposts-Bucket mithilfe eines mehrteiligen Uploads	94
Auflisten von Teilen eines Objekts in einem S3-on-Outposts-Bucket	96
Abrufen einer Liste der in Bearbeitung befindlichen mehrteiligen Uploads in einem S3-on-Outposts-Bucket	97
Presigned verwenden URLs	98
Einschränkung vordefinierter Funktionen URL	99
Wer kann einen vorsignierten erstellen URL	101
Wann überprüft S3 on Outposts das Ablaufdatum und die Uhrzeit eines vorab URL signierten?	102
Freigabe von Objekten	102
Hochladen eines Objekts	108
Amazon S3 auf Outposts mit lokalem Amazon EMR	113
Einen Amazon S3 on Outposts-Bucket erstellen	113
Erste Schritte bei der Nutzung von Amazon EMR mit Amazon S3 auf Outposts	115
Autorisierungs- und Authentifizierungs-Caching	120
Konfiguration des Autorisierungs- und Authentifizierungscaches	120
Die SigV4a-Signatur wird validiert	121
Sicherheit	122
Einrichtung IAM	123
Prinzipale für die Richtlinien von S3 on Outposts	125
ARNs für S3 on Outposts	125
Beispielrichtlinien für S3 on Outposts	127
Berechtigungen für Endpunkte	128
Serviceverknüpfte Rollen für S3 on Outposts	131
Datenverschlüsselung	131

AWS PrivateLink für S3 auf Outposts	131
Beschränkungen und Einschränkungen	133
Zugriff auf S3-on-Outposts-Schnittstellenendpunkte	133
Aktualisierung einer lokalen Konfiguration DNS	135
Einen Endpunkt erstellen VPC	135
VPCEndpunktrichtlinien und Bucket-Richtlinien erstellen	136
Signature Version 4 (SigV4) Richtlinienschlüssel	138
Beispiele für Bucket-Richtlinien, die mit der Signature Version 4 verbundene Bedingungsschlüssel verwenden	140
AWS verwaltete Richtlinien	142
AWSS3OnOutpostsServiceRolePolicy	143
Richtlinienaktualisierungen	143
Verwenden von serviceverknüpften Rollen	143
Berechtigungen von serviceverknüpften Rollen für S3 on Outposts	144
Erstellen einer serviceverknüpften Rolle für S3 on Outposts	147
Bearbeiten einer serviceverknüpften Rolle für S3 on Outposts	147
Löschen einer serviceverknüpften Rolle für S3 on Outposts	148
Unterstützte Regionen für serviceverknüpfte S3-on-Outposts-Rollen	148
Verwaltung von S3-on-Outposts-Speicher	149
Verwalten der S3-Versionsverwaltung	149
Erstellen und Verwalten einer Lebenszyklus-Konfiguration	152
Verwenden der Konsole	153
Verwenden von AWS CLI und SDK für Java	157
Replikation von Objekten für S3 in Outposts	161
Replikationskonfiguration	162
Anforderungen für S3 Replication in Outposts	163
Was wird repliziert?	163
Was wird nicht repliziert?	164
Was wird von S3 Replication in Outposts nicht unterstützt?	165
Einrichten der Replikation	165
Verwalten Ihrer Replikation	185
Freigabe von S3 on Outposts	194
Voraussetzungen	194
Verfahren	195
Verwendungsbeispiele	196
Sonstige -Services	199

Überwachen von S3 in Outposts	200
CloudWatch Metriken	200
CloudWatch Metriken	201
CloudWatch Amazon-Veranstaltungen	203
CloudTrail Logs	204
CloudTrail Protokollierung für S3 auf Outposts aktivieren	205
Einträge in der AWS CloudTrail Protokolldatei von Amazon S3 on Outposts	208
Entwickeln mit S3 on Outposts	211
S3 auf Outposts APIs	211
Amazon S3 API S3-Operationen zur Verwaltung von Objekten	211
Amazon S3 API Control-Operationen für die Verwaltung von Buckets	212
S3 on API Outposts-Operationen zur Verwaltung von Outposts	213
Konfigurieren des S3-Steuerungs-Clients	214
Senden von Anfragen über IPv6	214
Erste Schritte mit IPv6	215
Anforderungen unter Verwendung von Dual-Stack-Endpunkten	216
IPv6Adressen in IAM Richtlinien verwenden	217
Testen der IP-Adresskompatibilität	218
Verwenden mit IPv6 AWS PrivateLink	219
Verwenden von Dual-Stack-Endpunkten	222
.....	ccxxvii

Was ist Amazon S3 on Outposts?

AWS Outposts ist ein vollständig verwalteter Service, der dieselbe AWS Infrastruktur, dieselben AWS Services und Tools für praktisch jedes Rechenzentrum APIs, jeden Colocation-Bereich oder jede lokale Einrichtung bietet und so für ein wirklich konsistentes Hybrid-Erlebnis sorgt. AWS Outposts ist ideal für Workloads, die Zugriff auf lokale Systeme mit niedriger Latenz, lokale Datenverarbeitung, Datenresidenz und Migration von Anwendungen mit lokalen Systemabhängigkeiten erfordern. Weitere Informationen finden Sie unter [Was ist AWS Outposts?](#) im AWS Outposts -Benutzerhandbuch.

Mit Amazon S3 on Outposts können Sie S3-Buckets in Ihren Outposts erstellen und Objekte einfach On-Premises speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse `OUTPOSTS`, die Amazon S3 verwendet APIs und darauf ausgelegt ist, Daten dauerhaft und redundant auf mehreren Geräten und Servern in Ihren Outposts zu speichern. Sie kommunizieren mit Ihrem Outposts-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden.

Sie können für APIs Outposts-Buckets dieselben Funktionen wie für Amazon S3 verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden.

- [Funktionsweise von S3 on Outposts](#)
- [Funktionen von S3 on Outposts](#)
- [Zugehörige Services](#)
- [Zugriff auf S3 on Outposts](#)
- [Bezahlung für S3 on Outposts](#)
- [Nächste Schritte](#)

Funktionsweise von S3 on Outposts

S3 on Outposts ist ein Objektspeicherdienst, der Daten als Objekte in Buckets in Ihrem Outpost speichert. Ein Objekt ist eine Datendatei und alle Metadaten, die diese Datei beschreiben. Ein Bucket ist ein Container für Objekte.

Um Ihre Daten in S3 on Outposts zu speichern, müssen Sie zunächst einen Bucket erstellen. Beim Erstellen des Buckets geben Sie einen Bucket-Namen und den Outpost an, der den Bucket enthält. Um auf Ihren S3-on-Outposts-Bucket zuzugreifen und Objektoperationen durchzuführen, erstellen und konfigurieren Sie als Nächstes einen Zugriffspunkt. Sie müssen auch einen Endpunkt erstellen, um Anfragen an Ihren Zugriffspunkt weiterzuleiten.

Access Points vereinfachen den Datenzugriff für jede AWS-Service Kundenanwendung, die Daten in S3 speichert. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind und mit denen Sie Objektvorgänge ausführen können, z. B. GetObject und PutObject. Jeder Zugriffspunkt verfügt über unterschiedliche Berechtigungen und Netzwerkkontrollen.

Sie können Ihre S3 on Outposts Buckets, Access Points und Endpoints erstellen und verwalten, indem Sie AWS Management Console, AWS CLI, AWS SDKs oder verwenden. REST API Um Objekte in Ihren S3 on Outposts-Bucket hochzuladen und zu verwalten, können Sie das AWS CLI AWS SDKs, oder REST API verwenden.

Regionen

Während der AWS Outposts Bereitstellung erstellen Sie oder AWS erstellen eine Service Link-Verbindung, die Ihren Outpost für Bucket-Operationen und Telemetrie wieder mit der von Ihnen ausgewählten AWS-Region oder Outposts-Heimatregion verbindet. Ein Outpost ist auf Konnektivität zum übergeordneten AWS-Region angewiesen. Das Outposts-Rack ist nicht für getrennte Operationen oder Umgebungen mit eingeschränkter oder keiner Konnektivität ausgelegt. Weitere Informationen finden Sie unter [Outpost-Konnektivität zu AWS-Regionen](#) im AWS Outposts Benutzerhandbuch.

Buckets

Ein Bucket ist ein Behälter für Objekte, die in S3 on Outposts gespeichert werden. Sie können beliebig viele Objekte in einem Bucket speichern und bis zu 100 Buckets pro Konto in einem Outpost haben.

Wenn Sie einen Bucket erstellen, geben Sie einen Bucket-Namen ein und wählen den Outpost, in dem der Bucket angelegt werden soll. Der Name eines erstellten Buckets oder sein Outpost kann nicht nachträglich geändert werden. Bucket-Namen müssen den [Regeln für die Benennung von Amazon-S3-Buckets](#) folgen. In S3 on Outposts sind Bucket-Namen für einen Outpost und eindeutig. AWS-Kontooutpost-id, account-id und der Bucket-Name müssen die S3-on-Outposts-Buckets identifizieren.

Das folgende Beispiel zeigt das Amazon Resource Name (ARN) -Format für S3 in Outposts-Buckets. Das ARN besteht aus der Region, in der sich Ihr Outpost befindet, Ihrem Outpost-Konto, der Outpost-ID und dem Bucket-Namen.

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

Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point ARN oder Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das Access ARN Point-Format für S3 auf Outposts, das den `outpost-id` und `account-id`, und den Namen des Access Points umfasst:

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

Weitere Informationen über Buckets finden Sie unter [Arbeiten mit S3-on-Outposts-Buckets](#).

Objekte

Objekte sind die Grundeinheiten, die in S3 on Outposts gespeichert sind. Objekte bestehen aus Objekt- und Metadaten. Metadaten bestehen aus mehreren Name/Wert-Paaren, die das Objekt beschreiben. Diese Paare enthalten einige Standardmetadaten, wie das Datum der letzten Änderung, und HTTP Standardmetadaten wie `Content-Type`. Sie können bei der Speicherung des Objekts auch benutzerdefinierte Metadaten angeben. Ein Objekt wird innerhalb eines Buckets eindeutig durch einen Schlüssel (oder Namen) identifiziert.

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie AWS ein Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Schlüssel

Ein Objektschlüssel (oder Schlüsselname) ist der eindeutige Bezeichner für ein Objekt in einem Bucket. Jedes Objekt in einem Bucket besitzt genau einen Schlüssel. Jedes Objekt wird durch die Kombination aus Bucket und Objektschlüssel eindeutig identifiziert.

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Objekten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, ID, AWS-Konto Outpost-ID, Bucket-Namen und Objektschlüssel enthält:

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

Weitere Informationen über Objektschlüssel finden Sie unter [Arbeiten mit S3-on-Outposts-Objekten](#).

S3-Versioning

Sie können die S3-Versionsverwaltung für Outposts-Buckets verwenden, um mehrere Versionen eines Objekts im selben Bucket aufzubewahren. Mit S3-Versioning können Sie jede Version jedes in Ihren Buckets gespeicherten Objekts beibehalten, abrufen und wiederherstellen. Mit der S3-Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Weitere Informationen finden Sie unter [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#).

Versions-ID

Wenn Sie die S3-Versionsverwaltung in einem Bucket aktivieren, generiert S3 on Outposts eine eindeutige Versions-ID für jedes Objekt, das dem Bucket hinzugefügt wird. Objekte, die zum Zeitpunkt der Aktivierung des Versioning bereits im Bucket vorhanden waren, haben die Versions-ID null. Wenn Sie diese (oder andere) Objekte beispielsweise mit anderen Operationen ändern, erhalten die neuen Objekte eine eindeutige Versions-ID. [PutObject](#)

Weitere Informationen finden Sie unter [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#).

Speicherklasse und Verschlüsselung

S3 in Outposts bietet eine neue Speicherklasse: S3 Outposts (OUTPOSTS). Die Speicherklasse S3 Outposts ist nur für Objekte verfügbar, die in Buckets auf AWS Outposts gespeichert sind. Wenn Sie versuchen, andere S3-Speicherklassen mit S3 on Outposts zu verwenden, gibt S3 on Outposts den Fehler `InvalidStorageClass` aus.

Standardmäßig werden Objekte, die in der Speicherklasse S3 Outposts (OUTPOSTS) gespeichert sind, mit serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt. Weitere Informationen finden Sie unter [Datenverschlüsselung in S3 on Outposts](#).

Bucket-Richtlinie

Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) Richtlinie, mit der Sie Zugriffsberechtigungen für Ihren Bucket und die darin enthaltenen Objekte gewähren können. Nur der Bucket-Eigentümer kann einem Bucket eine Richtlinie zuordnen. Die dem Bucket zugeordneten Berechtigungen gelten für alle Objekte im Bucket, die dem Bucket-Eigentümer gehören. Bucket-Richtlinien sind auf eine Größe von 20 KB beschränkt.

Bucket-Richtlinien verwenden eine JSON auf IAM Richtlinien basierende Sprache, die überall Standard ist. AWS Sie können Bucket-Richtlinien verwenden, um Berechtigungen für die Objekte in einem Bucket hinzuzufügen oder zu verweigern. Bucket-Richtlinien erlauben oder verweigern Anforderungen basierend auf den Elementen in der Richtlinie. Diese Elemente können den Anforderer, S3-on-Outposts-Aktionen, Ressourcen und Aspekte oder Bedingungen der Anforderung beinhalten (z. B. die IP-Adresse, die für die Anforderung verwendet wird). Sie können beispielsweise eine Bucket-Richtlinie erstellen, die kontoübergreifende Berechtigungen zum Hochladen von Objekten in einen S3-on-Outposts-Bucket gewährt, während gleichzeitig sichergestellt wird, dass der Bucket-Eigentümer die volle Kontrolle über die hochgeladenen Objekte hat.

In Ihrer Bucket-Richtlinie können Sie Platzhalterzeichen (*) ARNs und andere Werte verwenden, um einer Teilmenge von Objekten Berechtigungen zu erteilen. Sie können beispielsweise den Zugriff auf Gruppen von Objekten steuern, die mit einem gemeinsamen [Präfix](#) beginnen oder mit einer bestimmten Erweiterung wie `.html` enden.

S3-on-Outposts-Zugriffspunkte

S3-on-Outposts-Zugriffspunkte sind benannte Netzwerkendpunkte mit dedizierten Zugriffsrichtlinien, die beschreiben, wie mit diesem Endpunkt auf Daten zugegriffen werden kann. Zugriffspunkte

vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in S3 on Outposts. Zugriffspunkte sind Buckets zugeordnet, mit denen Sie S3-Objektvorgänge ausführen können, z. B. `GetObject` und `PutObject`.

Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point ARN oder Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Jeder Zugriffspunkt verfügt über unterschiedliche Berechtigungen und Netzwerkkontrollen, die S3 on Outposts auf alle Anforderungen anwendet, die über diesen Zugriffspunkt eingehen. Jeder Zugriffspunkt erzwingt eine benutzerdefinierte Zugriffspunktrichtlinie, die in Verbindung mit der Bucket-Richtlinie funktioniert, die dem zugrunde liegenden Bucket zugeordnet ist.

Weitere Informationen finden Sie unter [Zugriff auf Ihre S3-on-Outposts-Buckets und -Objekte](#).

Funktionen von S3 on Outposts

Zugriffsverwaltung

S3 on Outposts bietet Funktionen für die Überwachung und Verwaltung des Zugriffs auf Ihre Buckets und Objekte. Standardmäßig werden S3-on-Outposts-Buckets und -Objekte als privat eingestuft. Sie haben nur Zugriff auf die S3-on-Outposts-Ressourcen, die Sie erstellen.

Um detaillierte Ressourcenberechtigungen zu erteilen, die Ihren speziellen Anwendungsfall unterstützen, oder um die Berechtigungen Ihrer S3-on-Outposts-Ressourcen zu überprüfen, können Sie die folgenden Funktionen verwenden.

- [S3 öffentlichen Zugriff blockieren](#) – Blockieren Sie den öffentlichen Zugriff auf Buckets und Objekte. Für Buckets auf Outposts ist „Öffentlichen Zugriff blockieren“ standardmäßig aktiviert.
- [AWS Identity and Access Management \(IAM\)](#) — IAM ist ein Webservice, mit dem Sie den Zugriff auf AWS Ressourcen, einschließlich Ihrer S3 on Outposts-Ressourcen, sicher kontrollieren können. Mit können Sie Berechtigungen zentral verwalten IAM, mit denen gesteuert wird, auf welche AWS Ressourcen Benutzer zugreifen können. Sie steuern IAM damit, wer authentifiziert (angemeldet) und autorisiert ist (über Berechtigungen verfügt), um Ressourcen zu verwenden.
- [S3-on-Outposts-Zugriffspunkte](#) – Verwalten Sie den Datenzugriff auf freigegebene Datensätze in S3 on Outposts. Zugriffspunkte sind benannte Netzwerkendpunkte mit dedizierten Zugriffsrichtlinien. Zugriffspunkte sind Buckets zugeordnet und können für Objektvorgänge verwendet werden, z. B. `GetObject` und `PutObject`.

- [Bucket-Richtlinien](#) — Verwenden Sie eine IAM basierte Richtlinienprache, um ressourcenbasierte Berechtigungen für Ihre S3-Buckets und die darin enthaltenen Objekte zu konfigurieren.
- [AWS Resource Access Manager \(AWS RAM\)](#) — Teilen Sie Ihre S3 on Outposts-Kapazität auf sichere Weise innerhalb Ihrer Organisation oder Ihrer Organisationseinheiten (OUs) in AWS Organizations. AWS-Konten

Speicherprotokollierung und Überwachung

S3 on Outposts bietet Protokollierungs- und Überwachungstools, mit denen Sie überwachen und steuern können, wie Ihre S3-on-Outposts-Ressourcen verwendet werden. Weitere Informationen finden Sie unter [Überwachungstools](#).

- [CloudWatch Amazon-Metriken für S3 on Outposts](#) — Verfolgen Sie den Betriebsstatus Ihrer Ressourcen und machen Sie sich ein Bild von Ihrer Kapazitätsverfügbarkeit.
- [Amazon CloudWatch Events-Ereignisse für S3 on Outposts](#) — Erstellen Sie eine Regel für jedes S3 on API Outposts-Ereignis, um Benachrichtigungen über alle unterstützten CloudWatch Events-Ziele zu erhalten, einschließlich Amazon Simple Queue Service (AmazonSQS), Amazon Simple Notification Service (AmazonSNS) und AWS Lambda
- [AWS CloudTrail Logs für S3 on Outposts](#) — Zeichnet Aktionen auf, die von einem Benutzer, einer Rolle oder einem AWS-Service in S3 auf Outposts ausgeführt wurden. CloudTrail Protokolle bieten Ihnen eine detaillierte API Nachverfolgung von S3-Vorgängen auf Bucket- und Objektebene.

Starke Konsistenz

S3 on Outposts bietet insgesamt eine hohe read-after-write Konsistenz für Objekte PUT und DELETE Anfragen von Objekten in Ihrem S3 on Outposts-Bucket. AWS-Regionen Dieses Verhalten gilt sowohl für Schreibvorgänge neuer Objekte als auch für PUT Anfragen, die bestehende Objekte überschreiben, und für Anfragen. DELETE Darüber hinaus sind Objekt-Tags und Objektmetadaten (z. B. das HEAD Objekt) in S3 on Outposts stark konsistent. Weitere Informationen finden Sie unter [Amazon S3 S3-Datenkonsistenzmodell](#) im Amazon S3 S3-Benutzerhandbuch.

Zugehörige Services

Nachdem Sie Daten in S3 on Outposts hochgeladen haben, können Sie sie mit anderen AWS-Services nutzen. Häufig genutzte Services:

- [Amazon Elastic Compute Cloud \(AmazonEC2\)](#) — Bietet sichere und skalierbare Rechenkapazität in der AWS Cloud. Durch die Verwendung von Amazon EC2 müssen Sie nicht im Voraus in Hardware investieren, sodass Sie Anwendungen schneller entwickeln und bereitstellen können. Sie können Amazon verwenden EC2, um so viele oder so wenige virtuelle Server wie nötig zu starten, Sicherheit und Netzwerke zu konfigurieren und Speicher zu verwalten.
- [Amazon Elastic Block Store \(AmazonEBS\) auf Outposts](#) — Verwenden Sie EBS lokale Amazon-Snapshots auf Outposts, um Snapshots von Volumes auf einem Outpost lokal in S3 auf Outposts zu speichern.
- [Amazon Relational Database Service \(AmazonRDS\) auf Outposts](#) — Verwenden Sie RDS lokale Amazon-Backups, um Ihre RDS Amazon-Backups lokal auf Ihrem Outpost zu speichern.
- [AWS DataSync](#) — Automatisieren Sie die Übertragung von Daten zwischen Ihren Outposts und entscheiden Sie AWS-Regionen, was übertragen werden soll, wann übertragen werden soll und wie viel Netzwerkbandbreite verwendet werden soll. S3 on Outposts ist integriert in. AWS DataSync Für On-Premises-Anwendungen, die eine lokale Verarbeitung mit hohem Durchsatz erfordern, bietet S3 on Outposts On-Premises-Objektspeicher, um Datenübertragungen zu minimieren und einen Puffer gegen Netzwerkschwankungen zu bieten, und ermöglicht Ihnen gleichzeitig, Daten einfach zwischen Outposts und AWS-Regionen zu übertragen.

Zugriff auf S3 on Outposts

Sie können mit S3 on Outposts auf eine der folgenden Arten arbeiten:

AWS Management Console

Die Konsole ist eine webbasierte Benutzeroberfläche für die Verwaltung von S3 on Outposts und AWS -Ressourcen. Wenn Sie sich für eine angemeldet haben AWS-Konto, können Sie auf S3 auf Outposts zugreifen, indem Sie sich bei der anmelden AWS Management Console und auf der AWS Management Console Startseite S3 auswählen. Wählen Sie dann Outposts buckets (Outposts-Buckets) aus dem linken Navigationsbereich aus.

AWS Command Line Interface

Sie können die AWS Befehlszeilentools verwenden, um Befehle auszugeben oder Skripte an der Befehlszeile Ihres Systems zu erstellen, um Aufgaben AWS (einschließlich S3) auszuführen.

Das [AWS Command Line Interface \(AWS CLI\)](#) bietet Befehle für eine Vielzahl von AWS-Services. Das AWS CLI wird unter Windows, MacOS und Linux unterstützt. Informationen zu den ersten

Schritten finden Sie im [AWS Command Line Interface -Benutzerhandbuch](#). Weitere Informationen zu den Befehlen, die Sie mit S3 on Outposts verwenden können, finden Sie unter [s3api](#), [s3control](#) und [s3outposts](#) in der AWS CLI -Befehlsreferenz.

AWS SDKs

AWS stellt SDKs (Software Development Kits) bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen (Java, Python, Ruby, .NET, iOS, Android usw.). AWS SDKs bieten eine bequeme Möglichkeit, programmatischen Zugriff auf S3 auf Outposts und zu erstellen. Da S3 on Outposts dasselbe verwendet SDKs wie Amazon S3, bietet S3 on Outposts ein einheitliches Erlebnis mit denselben S3 APIs, derselben Automatisierung und denselben Tools.

S3 on Outposts ist ein REST Service. Sie können Anfragen an S3 auf Outposts senden, indem Sie die AWS SDK Bibliotheken verwenden, die die zugrunde liegenden Daten zusammenfassen REST API und Ihre Programmieraufgaben vereinfachen. SDKs kümmern sich beispielsweise um Aufgaben wie das Berechnen von Signaturen, das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen. Informationen zu den AWS SDKs, einschließlich deren Herunterladen und Installieren, finden Sie unter [Tools, auf](#) denen Sie aufbauen können. AWS

Bezahlung für S3 on Outposts

Sie können eine Vielzahl von AWS Outposts Rack-Konfigurationen mit einer Kombination aus EC2 Amazon-Instance-Typen, Amazon EBS Allzweck-Solid-State-Laufwerken (SSD), Volumes (gp2) und S3 on Outposts erwerben. Die Preise beinhalten Lieferung, Installation, Wartung von Infrastruktur-Services sowie Softwarepatches und Upgrades.

Weitere Informationen finden Sie in der [Preisliste für AWS Outposts -Racks](#).

Nächste Schritte

Weitere Informationen zur Arbeit mit S3 on Outposts finden Sie in den folgenden Themen:

- [Einrichten Ihres Outposts](#)
- [Wie unterscheidet sich Amazon S3 on Outposts von Amazon S3?](#)
- [Erste Schritte mit Amazon S3 on Outposts](#)

- [Vernetzung für S3 on Outposts](#)
- [Arbeiten mit S3-on-Outposts-Buckets](#)
- [Arbeiten mit S3-on-Outposts-Objekten](#)
- [Sicherheit in S3 on Outposts](#)
- [Verwaltung von S3-on-Outposts-Speicher](#)
- [Entwickeln mit Amazon S3 on Outposts](#)

Einrichten Ihres Outposts

Um mit Amazon S3 on Outposts zu beginnen, benötigen Sie einen Outpost mit Amazon-S3-Kapazität, der in Ihrer Einrichtung bereitgestellt wird. Weitere Informationen zu den Optionen für die Bestellung eines Outposts und von S3-Kapazitäten finden Sie unter [AWS Outposts](#). Um zu überprüfen, ob Ihre Outposts über S3-Kapazität verfügen, können Sie den [ListOutpostsWithAPIS3-Anruf](#) verwenden. Technische Daten und weitere Informationen dazu, wie sich S3 on Outposts von Amazon S3 unterscheidet, finden Sie unter [Wie unterscheidet sich Amazon S3 on Outposts von Amazon S3?](#)

Weitere Informationen finden Sie unter den folgenden Themen.

Themen

- [Einen neuen -Outpost bestellen](#)

Einen neuen -Outpost bestellen

Wenn Sie einen neuen Outpost mit S3-Kapazität bestellen müssen, sehen Sie sich die [AWS Outposts Rackpreise](#) an, um mehr über die Kapazitätsoptionen für Amazon Elastic Compute Cloud (AmazonEC2), Amazon Elastic Block Store (AmazonEBS) und Amazon S3 zu erfahren.

Nach der Auswahl der Konfiguration führen Sie die Schritte unter [Erstellen eines Outposts und Bestellen von Outpost-Kapazitäten](#) im AWS Outposts -Benutzerhandbuch aus.

Wie unterscheidet sich Amazon S3 on Outposts von Amazon S3?

Amazon S3 on Outposts stellt Objektspeicher für Ihre lokale AWS Outposts Umgebung bereit. Mit S3 on Outposts können Sie die Anforderungen im Hinblick auf lokale Verarbeitung, Datenaufbewahrung und anspruchsvolle Leistung erfüllen, indem Daten in der Nähe von lokalen Anwendungen bleiben. Da S3 on Outposts Amazon S3 APIs und Funktionen nutzt, ist es ganz einfach, die Daten in Ihren Outposts zu speichern, zu sichern, zu kennzeichnen, darüber zu berichten und den Zugriff darauf zu kontrollieren und die AWS Infrastruktur auf Ihre lokale Einrichtung auszudehnen, um ein konsistentes Hybriderlebnis zu gewährleisten.

Weitere Informationen zu den Alleinstellungsmerkmalen von S3 on Outposts finden Sie in den folgenden Themen.

Themen

- [Spezifikationen für S3 auf Outposts](#)
- [API-Operationen, die von S3 auf Outposts unterstützt werden](#)
- [Amazon-S3-Funktionen, die von S3 auf Outposts nicht unterstützt werden](#)
- [Netzwerkanforderungen von S3 on Outposts](#)

Spezifikationen für S3 auf Outposts

- Die maximale Outpost-Bucket-Größe beträgt 50 TB.
- Die maximale Anzahl von Outpost-Buckets beträgt 100 pro AWS-Konto.
- Auf Outpost-Buckets kann nur über Zugriffs- und Endpunkte zugegriffen werden.
- Die maximale Anzahl von Zugriffspunkten pro Outpost-Bucket beträgt 10.
- Zugriffspunkt-Richtlinien sind auf eine Größe von 20 KB beschränkt.
- Der Outpost-Eigentümer kann den Zugriff innerhalb Ihrer Organisation mithilfe von AWS Organizations AWS Resource Access Manager Alle Konten, die Zugriff auf den Außenposten benötigen, müssen sich innerhalb derselben Organisation befinden wie das Eigentümerkonto in AWS Organizations.
- Das S3 in Outposts-Bucket-Eigentümerkonto ist immer der Eigentümer aller Objekte im Bucket.
- Nur das S3 in Outposts-Bucket-Eigentümerkonto kann Vorgänge für den Bucket ausführen.

- Die Objektgrößenbegrenzungen entsprechen denen von Amazon S3.
- Alle auf S3 auf Outposts gespeicherten Objekte werden in der Speicherklasse OUTPOSTS gespeichert.
- Standardmäßig werden alle in der OUTPOSTS Speicherklasse gespeicherten Objekte mithilfe serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) gespeichert. Sie können sich auch explizit dafür entscheiden, Objekte mithilfe einer serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (-C) zu speichern. SSE
- Wenn in Ihrem Outpost nicht genügend Speicherplatz zum Speichern eines Objekts vorhanden ist, wird eine Ausnahme mit unzureichender Kapazität () API zurückgegeben. ICE

API-Operationen, die von S3 auf Outposts unterstützt werden

Eine Liste der von S3 auf Outposts unterstützten API Operationen finden Sie unter [Betrieb von Amazon S3 bei Outposts API](#).

Amazon-S3-Funktionen, die von S3 auf Outposts nicht unterstützt werden

Mehrere Amazon-S3-Funktionen werden derzeit von Amazon S3 auf Outposts nicht unterstützt. Versuche, sie zu verwenden, werden zurückgewiesen.

- Zugriffskontrolllisten () ACLs
- Quellenübergreifende gemeinsame Nutzung von Ressourcen () CORS
- S3-BatchVorgänge
- S3-Bestandsberichte
- Ändern der Bucket-Standard-Verschlüsselung
- Öffentliche Buckets
- Multi-Faktor-Authentifizierung () löschen MFA
- S3-Lebenszyklusübergänge (abgesehen von der Objektlöschung und dem Abbrechen unvollständiger mehrteiliger Uploads)
- S3-Objektsperre aufgrund gesetzlicher Aufbewahrungsfristen
- Aufrechterhaltung der Objektsperre

- Serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) Schlüsseln (SSE-) KMS
- Steuerung der S3-Replikationszeit (S3RTC)
- CloudWatch Amazon-Anforderungskennzahlen
- Metrik-Konfiguration
- Transfer Acceleration
- S3-Ereignis-Benachrichtigungen
- Buckets mit Zahlung durch den Anforderer
- S3 Select
- AWS Lambda Ereignisse
- Server access logging (Server-Zugriffsprotokollierung)
- HTTPPOSTAnfragen
- SOAP
- Websitezugriff

Netzwerkanforderungen von S3 on Outposts

- Um Anforderungen an einen Zugriffspunkt für S3 in Outposts weiterzuleiten, müssen Sie einen S3-in-Outposts-Endpunkt erstellen und konfigurieren. Für Endpunkte für S3 in Outposts gelten die folgenden Beschränkungen:
 - Jeder virtuellen privaten Cloud (VPC) in einem Outpost kann ein Endpunkt zugeordnet sein, und Sie können bis zu 100 Endpunkte pro Outpost haben.
 - Sie können einem Endpunkt mehrere Zugriffspunkte zuordnen.
 - Sie können Endpunkte nur VPCs mit CIDR Blöcken in den Unterräumen der folgenden Bereiche hinzufügen: CIDR
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
 - Sie können nur Endpunkte für einen Außenposten erstellen, deren Blöcke VPCs sich nicht überschneiden. CIDR
 - Sie können einen Endpunkt nur aus seinem Outposts-Subnetz erstellen.

- Das Subnetz, das Sie zum Erstellen eines Endpunkts verwenden, muss vier IP-Adressen enthalten, die S3 in Outposts verwenden kann.
- Wenn Sie den kundeneigenen IP-Adresspool (CoIP-Pool) angeben, muss dieser vier IP-Adressen enthalten, die S3 in Outposts verwenden kann.
- Sie können nur einen Endpunkt pro Außenposten pro erstellen. VPC

Erste Schritte mit Amazon S3 on Outposts

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden.

Mit Amazon S3 on Outposts können Sie Amazon S3 APIs und Funktionen wie Objektspeicher, Zugriffsrichtlinien, Verschlüsselung und Tagging genauso nutzen AWS Outposts wie in Amazon S3. Weitere Informationen zu S3 on Outposts finden Sie unter [Was ist Amazon S3 on Outposts?](#).

Themen

- [Erste Schritte mit der AWS Management Console](#)
- [Erste Schritte mit der Verwendung von AWS CLI und SDK für Java](#)

Erste Schritte mit der AWS Management Console

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Weitere Informationen zu den ersten Schritten mit S3 on Outposts unter Verwendung der Konsole finden Sie in den folgenden Themen. Informationen zu den ersten Schritten mit dem AWS CLI oder finden Sie AWS SDK for Java unter [Erste Schritte mit der Verwendung von AWS CLI und SDK für Java](#).

Themen

- [Einen Bucket, einen Zugriffspunkt und einen Endpunkt erstellen](#)
- [Nächste Schritte](#)

Einen Bucket, einen Zugriffspunkt und einen Endpunkt erstellen

Die folgende Vorgehensweise veranschaulicht, wie Sie Ihren ersten Bucket in S3 on Outposts erstellen können. Wenn Sie einen Bucket mit der Konsole erstellen, erstellen Sie auch einen Zugriffspunkt und einen Endpunkt, die mit dem Bucket verknüpft sind, sodass Sie sofort mit dem Speichern von Objekten in Ihrem Bucket beginnen können.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie Outposts-Bucket erstellen.
4. Geben Sie als Bucket-Namen einen Domain Name System (DNS) -kompatiblen Namen für Ihren Bucket ein.

Der Bucket-Name ...:

- Seien Sie einzigartig innerhalb des AWS-Konto Außenpostens und des Ortes, in dem der AWS-Region Außenposten beheimatet ist.
- Er muss zwischen 3 und 63 Zeichen lang sein.
- Enthält keine Großbuchstaben.
- mit einem Kleinbuchstaben oder einer Zahl beginnen.

Der Name eines einmal erstellter Buckets kann nicht nachträglich geändert werden.

Informationen zur Benennung von Buckets finden Sie unter [Allgemeine Benennungsregeln für Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

⚠ Important

Vermeiden Sie, vertrauliche Informationen, wie Kontonummern, in den Bucket-Namen einzubeziehen. Der Bucket-Name ist in dem Punkt sichtbarURLs, auf den die Objekte im Bucket verweisen.

5. Wählen Sie unter Outpost den Outpost aus, in dem sich der Bucket befinden soll.
6. Legen Sie unter Bucket Versioning (Bucket-Versionsverwaltung) den S3-Versionsverwaltungsstatus für Ihren S3-on-Outposts-Bucket auf eine der folgenden Optionen fest:
 - Disable (Deaktivieren) (Standard) – Der Bucket wird nicht versioniert.
 - Enable (Aktivieren) – Aktiviert die S3-Versionsverwaltung für die Objekte im Bucket. Alle Objekte, die dem Bucket hinzugefügt werden, erhalten eine eindeutige Versions-ID.

Weitere Informationen über das S3-Versioning finden Sie unter [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#).

7. (Optional) Fügen Sie ggf. optional tags (optionale Markierungen) hinzu, die Sie mit dem Outposts-Bucket verknüpfen möchten. Sie können Markierungen nutzen, um Kriterien für einzelne Projekte oder Gruppen von Projekten nachzuverfolgen oder um Ihre Buckets unter Verwendung der Kostenzuordnungs-Markierungen zu kennzeichnen.

Standardmäßig werden alle in Ihrem Outposts-Bucket gespeicherten Objekte mithilfe serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) gespeichert. Sie können sich auch explizit dafür entscheiden, Objekte zu speichern, indem Sie serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (-C) verwenden. SSE Um den Verschlüsselungstyp zu ändern, müssen Sie RESTAPI, AWS Command Line Interface (AWS CLI) oder verwenden. AWS SDKs

8. Geben Sie im Abschnitt Einstellungen für den Zugriffspunkt für Outposts den Namen des Zugriffspunkts ein.

S3-on-Outposts-Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in S3 on Outposts. Zugriffspunkte sind benannte Netzwerkendpunkte, die Outposts-Buckets zugeordnet sind, mit denen Sie S3-Objektoperationen ausführen können. Weitere Informationen finden Sie unter [Zugriffspunkte](#).

Die Namen der Access Points müssen innerhalb des Kontos für diese Region und diesen Outpost eindeutig sein und den [Einschränkungen und Beschränkungen der Access Points](#) entsprechen.

9. Wählen Sie VPC dafür den Amazon S3 on Outposts Access Point.

Wenn Sie noch keinen haben VPC, wählen Sie Create VPC. Weitere Informationen finden Sie unter [Erstellen von Zugriffspunkten, die auf eine virtuelle private Cloud beschränkt sind \(VPC\)](#) im Amazon S3 S3-Benutzerhandbuch.

Eine virtuelle private Cloud (VPC) ermöglicht es Ihnen, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

10. (Optional für ein vorhandenes VPC) Wählen Sie ein Endpunkt-Subnetz für Ihren Endpunkt.

Ein Subnetz ist ein Bereich von IP-Adressen in Ihrem VPC. Wenn Sie nicht das gewünschte Subnetz haben, wählen Sie Subnetz erstellen. Weitere Informationen finden Sie unter [Vernetzung für S3 on Outposts](#).

11. (Optional für ein vorhandenes VPC) Wählen Sie eine Endpunkt-Sicherheitsgruppe für Ihren Endpunkt aus.

Eine [Sicherheitsgruppe](#) dient als virtuelle Firewall zur Steuerung von ein- und ausgehendem Datenverkehr.

12. (Optional für einen vorhandenen VPC) Wählen Sie den Endpunktzugriffstyp:

- Privat — Zur Verwendung mit dem VPC.
- IP im Besitz des Kunden – Zur Verwendung mit einem kundeneigenen IP-Adresspool (CoIP-Pool) Ihres On-Premises-Netzwerks.

13. (Optional) Geben Sie die Outpost access point policy (Outpost-Zugriffspunkt-Richtlinie) an. Die Konsole zeigt automatisch den Amazon-Ressourcennamen (ARN) für den Access Point an, den Sie in der Richtlinie verwenden können.

14. Wählen Sie Outposts-Bucket erstellen.

Note

Es kann bis zu 5 Minuten dauern, bis der Outpost-Endpoint erstellt und der Bucket einsatzbereit ist. Um zusätzliche Bucket-Einstellungen zu konfigurieren, wählen Sie Details anzeigen.

Nächste Schritte

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn ein Outpost-Rack AWS installiert wird, bleiben Ihre Daten lokal in Ihrem Outpost gespeichert, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Nachdem Sie einen S3 on Outposts Bucket, Access Point und Endpoint erstellt haben, können Sie das AWS CLI oder SDK für Java verwenden, um ein Objekt in Ihren Bucket hochzuladen. Weitere Informationen finden Sie unter [Laden Sie ein Objekt in einen S3-Bucket auf Outposts hoch](#).

Erste Schritte mit der Verwendung von AWS CLI und SDK für Java

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Für die ersten Schritte mit S3 on Outposts müssen Sie einen Bucket, einen Zugriffspunkt und einen Endpunkt erstellen. Anschließend können Sie Ihre Objekte in den Bucket hochladen. Die folgenden

Beispiele zeigen Ihnen, wie Sie mit S3 auf Outposts beginnen können, indem Sie AWS CLI und SDK für Java verwenden. Die ersten Schritte mit der Konsole finden Sie unter [Erste Schritte mit der AWS Management Console](#).

Themen

- [Schritt 1: Erstellen eines Buckets](#)
- [Schritt 2: Erstellen eines Zugriffspunkts](#)
- [Schritt 3: Erstellen eines Endpunkts](#)
- [Schritt 4: Hochladen eines Objekts in einen S3-on-Outposts-Bucket](#)

Schritt 1: Erstellen eines Buckets

Die folgenden Beispiele AWS CLI und Beispiele SDK für Java zeigen Ihnen, wie Sie einen S3 on Outposts-Bucket erstellen.

AWS CLI

Example

Im folgenden Beispiel wird ein S3-on-Outposts-Bucket (`s3-outposts:CreateBucket`) mithilfe der AWS CLI erstellt. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

SDK for Java

Example

Im folgenden Beispiel wird mithilfe von SDK for Java ein S3 on Outposts Bucket (`s3-outposts:CreateBucket`) erstellt.

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

public String createBucket(String bucketName) {

    CreateBucketRequest reqCreateBucket = new CreateBucketRequest()
        .withBucket(bucketName)
        .withOutpostId(OutpostId)
```

```
        .withCreateBucketConfiguration(new CreateBucketConfiguration());

        CreateBucketResult respCreateBucket =
s3ControlClient.createBucket(reqCreateBucket);
        System.out.printf("CreateBucket Response: %s%n", respCreateBucket.toString());

        return respCreateBucket.getBucketArn();
    }
}
```

Schritt 2: Erstellen eines Zugriffspunkts

Um auf Ihren Amazon-S3-on-Outposts-Bucket zuzugreifen, müssen Sie einen Zugriffspunkt erstellen und konfigurieren. In diesen Beispielen erfahren Sie, wie Sie einen Access Point mithilfe von AWS CLI und SDK für Java erstellen.

Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in Amazon S3. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind, mit denen Sie Amazon S3-Objekt-Vorgänge ausführen können, z. B. `GetObject` und `PutObject`. Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Access Points unterstützen nur virtual-host-style Adressierung.

AWS CLI

Example

Im folgenden AWS CLI Beispiel wird ein Access Point für einen Outposts-Bucket erstellt. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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

Das folgende Beispiel SDK für Java erstellt einen Access Point für einen Outposts-Bucket. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

public String createAccessPoint(String bucketArn, String accessPointName) {

    CreateAccessPointRequest reqCreateAP = new CreateAccessPointRequest()
        .withAccountId(AccountId)
        .withBucket(bucketArn)
        .withName(accessPointName)
        .withVpcConfiguration(new VpcConfiguration().withVpcId("vpc-12345"));

    CreateAccessPointResult respCreateAP =
s3ControlClient.createAccessPoint(reqCreateAP);
    System.out.printf("CreateAccessPoint Response: %s%n", respCreateAP.toString());

    return respCreateAP.getAccessPointArn();
}
```

Schritt 3: Erstellen eines Endpunkts

Wenn Sie Anforderungen an einen Zugriffspunkt für Amazon S3 on Outposts weiterleiten möchten, müssen Sie einen S3-on-Outposts-Endpunkt erstellen und konfigurieren. Zum Erstellen eines Endpunkts muss Ihr Service-Link eine aktive Verbindung mit Ihrer Outposts-Heimatregion aufweisen. Jeder virtuellen privaten Cloud (VPC) auf Ihrem Outpost kann ein Endpunkt zugeordnet sein. Weitere Informationen zu Endpunktkontingenten finden Sie unter [Netzwerkanforderungen von S3 on Outposts](#). Sie müssen einen Endpunkt erstellen, um auf Ihre Outposts-Buckets zugreifen und Objekt-Operationen ausführen zu können. Weitere Informationen finden Sie unter [Endpunkte](#).

Diese Beispiele zeigen Ihnen, wie Sie mit dem AWS CLI und dem SDK für Java einen Endpunkt erstellen. Weitere Informationen zu den erforderlichen Berechtigungen für das Erstellen und Verwalten von Endpunkten finden Sie unter [Berechtigungen für S3-on-Outposts-Endpunkte](#).

AWS CLI

Example

Im folgenden AWS CLI Beispiel wird mithilfe des VPC Ressourcenzugriffstyps ein Endpunkt für einen Outpost erstellt. Der VPC wird aus dem Subnetz abgeleitet. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Im folgenden AWS CLI Beispiel wird mithilfe des Zugriffstyps des kundeneigenen IP-Adresspools (CoIP-Pool) ein Endpunkt für einen Outpost erstellt. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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

Das folgende Beispiel SDK für Java erstellt einen Endpunkt für einen Outpost. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
import com.amazonaws.services.s3outposts.AmazonS3Outposts;  
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;  
import com.amazonaws.services.s3outposts.model.CreateEndpointRequest;  
import com.amazonaws.services.s3outposts.model.CreateEndpointResult;  
  
public void createEndpoint() {  
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder  
        .standard().build();  
  
    CreateEndpointRequest createEndpointRequest = new CreateEndpointRequest()  
        .withOutpostId("op-0d79779cef3c30a40")  
        .withSubnetId("subnet-8c7a57c5")  
        .withSecurityGroupId("sg-ab19e0d1")  
        .withAccessType("CustomerOwnedIp")  
        .withCustomerOwnedIpv4Pool("ipv4pool-coip-12345678901234567");  
    // Use .withAccessType and .withCustomerOwnedIpv4Pool only when the access type  
    is  
    // customer-owned IP address pool (CoIP pool)  
    CreateEndpointResult createEndpointResult =  
s3OutpostsClient.createEndpoint(createEndpointRequest);  
    System.out.println("Endpoint is created and its ARN is " +  
createEndpointResult.getEndpointArn());  
}
```

}

Schritt 4: Hochladen eines Objekts in einen S3-on-Outposts-Bucket

Informationen zum Hochladen eines Objekts finden Sie unter [Laden Sie ein Objekt in einen S3-Bucket auf Outposts hoch](#).

Vernetzung für S3 on Outposts

Sie können Amazon S3 on Outposts verwenden, um Objekte lokal für Anwendungen zu speichern und abzurufen, die lokalen Datenzugriff, Datenverarbeitung und Datenresidenz erfordern. In diesem Abschnitt werden die Netzwerkanforderungen für den Zugriff auf S3 on Outposts beschrieben.

Themen

- [Auswählen des Netzwerkzugriffstyps](#)
- [Zugriff auf Ihre S3-on-Outposts-Buckets und -Objekte](#)
- [Kontenübergreifende Elastic-Netzwerk-Schnittstellen](#)

Auswählen des Netzwerkzugriffstyps

Sie können innerhalb eines VPC oder von Ihrem lokalen Netzwerk aus auf S3 on Outposts zugreifen. Sie kommunizieren mit Ihrem Outposts-Bucket über einen Zugriffspunkt und eine Endpunktverbindung. Diese Verbindung hält den Verkehr zwischen Ihnen VPC und Ihren S3 in Outposts-Buckets innerhalb des AWS Netzwerks aufrecht. Wenn Sie einen Endpunkt erstellen, müssen Sie den Endpunkt-Zugriffstyp entweder als `Private` (für VPC Routing) oder `CustomerOwnedIp` (für einen kundeneigenen IP-Adresspool [CoIP-Pool]) angeben.

- `Private`(für VPC Routing) — Wenn Sie den Zugriffstyp nicht angeben, verwendet S3 on Outposts `Private` standardmäßig. Bei diesem `Private` Zugriffstyp benötigen Ihre Instanzen VPC keine öffentlichen IP-Adressen, um mit Ressourcen in Ihrem Outpost zu kommunizieren. Sie können mit S3 auf Outposts von A VPC aus arbeiten. Auf diesen Endpunkttyp kann von Ihrem lokalen Netzwerk aus über direktes VPC Routing zugegriffen werden. Weitere Informationen finden Sie unter [Roouting-Tabellen für lokale Gateways](#) im AWS -Outposts-Benutzerhandbuch.
- `CustomerOwnedIp`(für CoIP-Pool) – Wenn Sie den Zugriffstyp `Private` nicht standardmäßig verwenden und `CustomerOwnedIp` auswählen, müssen Sie einen IP-Adressbereich angeben. Sie können diesen Zugriffstyp verwenden, um mit S3 auf Outposts sowohl von Ihrem lokalen Netzwerk als auch innerhalb eines zu arbeiten. VPC Wenn Sie auf S3 auf Outposts innerhalb von a zugreifenVPC, ist Ihr Datenverkehr auf die Bandbreite des lokalen Gateways beschränkt.

Zugriff auf Ihre S3-on-Outposts-Buckets und -Objekte

Um auf Ihre S3 on Outposts-Buckets und -Objekte zugreifen zu können, benötigen Sie Folgendes:

- Ein Zugangspunkt für die VPC.
- Ein Endpunkt für dasselbe VPC.
- Eine aktive Verbindung zwischen Ihrem Outpost und Ihrer AWS-Region. Weitere Informationen darüber, wie du deinen Outpost mit einer Region verbindest, findest du unter [Outpost-Konnektivität zu AWS Regionen](#) im AWS Outposts User Guide.

Weitere Informationen zum Zugriff auf Buckets und Objekte in S3 on Outposts finden Sie unter [Arbeiten mit S3-on-Outposts-Buckets](#) und [Arbeiten mit S3-on-Outposts-Objekten](#).

Kontenübergreifende Elastic-Network-Schnittstellen

S3 auf Outposts-Endpunkten sind benannte Ressourcen mit Amazon Resource Names (ARNs). Wenn diese Endpunkte erstellt werden, AWS Outposts werden mehrere kontenübergreifende elastische Netzwerkschnittstellen eingerichtet. Die kontenübergreifenden Elastic Network-Schnittstellen von S3 on Outposts sind wie andere Netzwerkschnittstellen mit einer Ausnahme: S3 on Outposts ordnet die kontenübergreifenden Elastic Network-Schnittstellen Amazon-Instances zu. EC2

Das S3 on Outposts Domain Name System (DNS) verteilt Ihre Anfragen über die kontenübergreifende elastic network interface. S3 on Outposts erstellt die kontenübergreifende elastic network interface in Ihrem AWS Konto, die im Bereich Netzwerkschnittstellen der EC2 Amazon-Konsole sichtbar ist.

Für Endpunkte, die den CoIP-Pool-Zugriffstyp verwenden, weist S3 on Outposts IP-Adressen der kontenübergreifenden Elastic-Network-Schnittstelle aus dem konfigurierten CoIP-Pool zu und ordnet sie dieser zu.

Arbeiten mit S3-on-Outposts-Buckets

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihrem Computer erstellen AWS Outposts und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Sie kommunizieren mit Ihren Outpost-Buckets, indem Sie einen Zugriffspunkt und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Um auf Ihre S3 on Outposts-Buckets und -Objekte zugreifen zu können, benötigen Sie einen Access Point für die VPC und einen Endpunkt dafür. Weitere Informationen finden Sie unter [Vernetzung für S3 on Outposts](#).

Buckets

In S3 on Outposts sind Bucket-Namen für einen Outpost eindeutig und erfordern den AWS-Region Code für die Region, in der sich der Outpost befindet, die AWS-Konto ID, die Outpost-ID und den Bucket-Namen, um sie zu identifizieren.

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

Weitere Informationen finden Sie unter [Ressource ARNs für S3 auf Outposts](#).

Zugriffspunkte

Amazon S3 on Outposts unterstützt ausschließlich virtuelle private Cloud-Zugriffspunkte (VPC) als einzige Möglichkeit, auf Ihre Outposts-Buckets zuzugreifen.

Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in Amazon S3. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind, mit denen Sie Amazon S3-Objekt-Vorgänge ausführen können, z. B. GetObject und PutObject. Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Access Points unterstützen nur Adressierung. virtual-host-style

Das folgende Beispiel zeigt das ARN Format, das Sie für S3 auf Outposts-Zugriffspunkten verwenden. Der Access Point ARN enthält den AWS-Region Code für die Region, in der sich der Outpost befindet, die AWS-Konto ID, die Outpost-ID und den Namen des Access Points.

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

Endpunkte

Um Anforderungen an einen Zugriffspunkt für S3 on Outposts weiterzuleiten, müssen Sie einen S3-on-Outposts-Endpunkt erstellen und konfigurieren. Mit S3 auf Outposts-Endpunkten können Sie Ihren Bucket privat mit Ihrem VPC Outpost-Bucket verbinden. S3 on Outposts-Endpunkte sind virtuelle einheitliche Ressourcen-Identifikatoren (URIs) des Einstiegspunkts zu Ihrem S3 on Outposts-Bucket. Es handelt sich um horizontal skalierte, redundante und hochverfügbare Komponenten. VPC

Jeder virtuellen privaten Cloud (VPC) auf Ihrem Outpost kann ein zugeordneter Endpunkt zugeordnet sein, und Sie können bis zu 100 Endpunkte pro Outpost haben. Sie müssen diese Endpunkte erstellen, um auf Ihren Outpost-Bucket zugreifen und Objektvorgänge ausführen zu können. Durch die Erstellung dieser Endpunkte können API Modell und Verhalten auch identisch sein, da dieselben Operationen in S3 und S3 auf Outposts ausgeführt werden können.

API Operationen auf S3 auf Outposts

Um API Outpost-Bucket-Operationen zu verwalten, hostet S3 on Outposts einen separaten Endpunkt, der sich vom Amazon S3 S3-Endpunkt unterscheidet. Dieser Endpunkt ist `s3-outposts.region.amazonaws.com`.

Um Amazon S3 API S3-Operationen verwenden zu können, müssen Sie den Bucket und die Objekte im richtigen ARN Format signieren. Sie müssen ARNs zu API Operations übergeben, damit Amazon S3 feststellen kann, ob es sich um eine Anfrage für Amazon S3 (`s3-control.region.amazonaws.com`) oder für S3 on Outposts (`s3-outposts.region.amazonaws.com`) handelt. Basierend auf dem ARN Format kann S3 die Anfrage dann entsprechend signieren und weiterleiten.

Immer wenn eine Anfrage an die Amazon S3 S3-Steuerebene gesendet wird, SDK extrahiert die die Komponenten aus der ARN und schließt den zusätzlichen Header ein `x-amz-outpost-id`, wobei der `outpost-id` Wert aus dem extrahiert wird ARN. Der Dienstname von ARN wird verwendet, um die Anfrage zu signieren, bevor sie an den Endpunkt S3 on Outposts weitergeleitet wird. Dieses Verhalten gilt für alle vom Client API abgewickelten Operationen. `s3control`

In der folgenden Tabelle sind die erweiterten API Operationen für Amazon S3 auf Outposts und ihre Änderungen im Vergleich zu Amazon S3 aufgeführt.

API	S3-on-Outposts-Parameterwert
CreateBucket	Bucket-Name alsARN, Outpost-ID
ListRegionalBuckets	Outpost-ID
DeleteBucket	Bucket-Name als ARN
DeleteBucketLifecycleConfiguration	Bucket-Name als ARN
GetBucketLifecycleConfiguration	Bucket-Name als ARN
PutBucketLifecycleConfiguration	Bucket-Name als ARN
GetBucketPolicy	Bucket-Name als ARN
PutBucketPolicy	Bucket-Name als ARN
DeleteBucketPolicy	Bucket-Name als ARN
GetBucketTagging	Bucket-Name als ARN
PutBucketTagging	Bucket-Name als ARN
DeleteBucketTagging	Bucket-Name als ARN
CreateAccessPoint	Name des Zugriffspunkts als ARN
DeleteAccessPoint	Name des Zugangspunkts als ARN
GetAccessPoint	Name des Zugangspunkts als ARN
GetAccessPoint	Name des Zugangspunkts als ARN
ListAccessPoints	Name des Zugangspunkts als ARN

API	S3-on-Outposts-Parameterwert
PutAccessPointPolicy	Name des Zugangspunkts als ARN
GetAccessPointPolicy	Name des Zugangspunkts als ARN
DeleteAccessPointPolicy	Name des Zugangspunkts als ARN

Erstellen und Verwalten von S3 on Outposts-Buckets

Weitere Informationen zum Erstellen und Verwalten von S3-on-Outposts-Buckets finden Sie in den folgenden Themen.

Erstellen eines S3-on-Outposts-Buckets

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. VPC Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Note

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der Aktionen für ihn ausführen kann. Buckets verfügen über Konfigurationseigenschaften wie Outpost, Tags, Standard-Verschlüsselung und Zugriffspunkteinstellungen. Zu den Zugriffspunkteinstellungen gehören die virtuelle private Cloud (VPC), die Zugriffspunktrichtlinie für den Zugriff auf die Objekte im Bucket und andere Metadaten. Weitere Informationen finden Sie unter [Spezifikationen für S3 auf Outposts](#).

Wenn Sie einen Bucket erstellen möchten, der Bucket- und Endpoint Management-Zugriff über VPC-Schnittstellenendpunkte in Ihrer Virtual Private Cloud (VPC) ermöglicht, finden Sie Informationen [AWS PrivateLink zu S3 auf Outposts](#). AWS PrivateLink

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe von, AWS Command Line Interface (AWS CLI) und AWS SDK for Java einen S3 on AWS Management Console Outposts-Bucket erstellen.

Verwenden der S3-Konsole

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie Outposts-Bucket erstellen.
4. Geben Sie als Bucket-Namen einen Domain Name System (DNS) -kompatiblen Namen für Ihren Bucket ein.

Der Bucket-Name ...:

- Seien Sie einzigartig innerhalb des AWS-Konto Außenpostens und des Ortes, in dem der AWS-Region Außenposten beheimatet ist.
- Er muss zwischen 3 und 63 Zeichen lang sein.
- Enthält keine Großbuchstaben.
- mit einem Kleinbuchstaben oder einer Zahl beginnen.

Der Name eines einmal erstellter Buckets kann nicht nachträglich geändert werden.

Informationen zur Benennung von Buckets finden Sie unter [Allgemeine Benennungsregeln für Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

Important

Vermeiden Sie, vertrauliche Informationen, wie Kontonummern, in den Bucket-Namen einzubeziehen. Der Bucket-Name ist in dem Punkt sichtbarURLs, auf den die Objekte im Bucket verweisen.

5. Wählen Sie unter Outpost den Outpost aus, in dem sich der Bucket befinden soll.

6. Legen Sie unter Bucket Versioning (Bucket-Versionsverwaltung) den S3-Versionsverwaltungsstatus für Ihren S3-on-Outposts-Bucket auf eine der folgenden Optionen fest:

- Disable (Deaktivieren) (Standard) – Der Bucket wird nicht versioniert.
- Enable (Aktivieren) – Aktiviert die S3-Versionsverwaltung für die Objekte im Bucket. Alle Objekte, die dem Bucket hinzugefügt werden, erhalten eine eindeutige Versions-ID.

Weitere Informationen über das S3-Versioning finden Sie unter [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#).

7. (Optional) Fügen Sie ggf. optional tags (optionale Markierungen) hinzu, die Sie mit dem Outposts-Bucket verknüpfen möchten. Sie können Markierungen nutzen, um Kriterien für einzelne Projekte oder Gruppen von Projekten nachzuverfolgen oder um Ihre Buckets unter Verwendung der Kostenzuordnungs-Markierungen zu kennzeichnen.

Standardmäßig werden alle in Ihrem Outposts-Bucket gespeicherten Objekte mithilfe serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) gespeichert. Sie können sich auch explizit dafür entscheiden, Objekte zu speichern, indem Sie serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (-C) verwenden. SSE Um den Verschlüsselungstyp zu ändern, müssen Sie RESTAPI, AWS Command Line Interface (AWS CLI) oder verwenden. AWS SDKs

8. Geben Sie im Abschnitt Einstellungen für den Zugriffspunkt für Outposts den Namen des Zugriffspunkts ein.

S3-on-Outposts-Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in S3 on Outposts. Zugriffspunkte sind benannte Netzwerkendpunkte, die Outposts-Buckets zugeordnet sind, mit denen Sie S3-Objektoperationen ausführen können. Weitere Informationen finden Sie unter [Zugriffspunkte](#).

Die Namen der Access Points müssen innerhalb des Kontos für diese Region und diesen Outpost eindeutig sein und den [Einschränkungen und Beschränkungen der Access Points](#) entsprechen.

9. Wählen Sie VPC dafür den Amazon S3 on Outposts Access Point.

Wenn Sie noch keinen haben VPC, wählen Sie Create VPC. Weitere Informationen finden Sie unter [Erstellen von Zugriffspunkten, die auf eine virtuelle private Cloud beschränkt sind \(VPC\)](#) im Amazon S3 S3-Benutzerhandbuch.

Eine virtuelle private Cloud (VPC) ermöglicht es Ihnen, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, kann jedoch die Vorteile der skalierbaren Infrastruktur von AWS nutzen.

10. (Optional für ein vorhandenes VPC) Wählen Sie ein Endpunkt-Subnetz für Ihren Endpunkt.

Ein Subnetz ist ein Bereich von IP-Adressen in Ihrem VPC. Wenn Sie nicht das gewünschte Subnetz haben, wählen Sie Subnetz erstellen. Weitere Informationen finden Sie unter [Vernetzung für S3 on Outposts](#).

11. (Optional für ein vorhandenes VPC) Wählen Sie eine Endpunkt-Sicherheitsgruppe für Ihren Endpunkt.


Eine [Sicherheitsgruppe](#) dient als virtuelle Firewall zur Steuerung von ein- und ausgehendem Datenverkehr.

12. (Optional für einen vorhandenen VPC) Wählen Sie den Endpunktzugriffstyp:

- Privat — Zur Verwendung mit dem VPC.
- IP im Besitz des Kunden – Zur Verwendung mit einem kundeneigenen IP-Adresspool (CoIP-Pool) Ihres On-Premises-Netzwerks.

13. (Optional) Geben Sie die Outpost access point policy (Outpost-Zugriffspunkt-Richtlinie) an. Die Konsole zeigt automatisch den Amazon-Ressourcennamen (ARN) für den Access Point an, den Sie in der Richtlinie verwenden können.

14. Wählen Sie Outposts-Bucket erstellen.

 Note

Es kann bis zu 5 Minuten dauern, bis der Outpost-Endpunkt erstellt und der Bucket einsatzbereit ist. Um zusätzliche Bucket-Einstellungen zu konfigurieren, wählen Sie Details anzeigen.

Mit dem AWS CLI

Example

Im folgenden Beispiel wird ein S3-on-Outposts-Bucket (`s3-outposts:CreateBucket`) mithilfe der AWS CLI erstellt. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Verwendung des AWS SDK for Java

Example

Im folgenden Beispiel wird mithilfe von SDK for Java ein S3 on Outposts Bucket (`s3-outposts:CreateBucket`) erstellt.

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

public String createBucket(String bucketName) {

    CreateBucketRequest reqCreateBucket = new CreateBucketRequest()
        .withBucket(bucketName)
        .withOutpostId(OutpostId)
        .withCreateBucketConfiguration(new CreateBucketConfiguration());

    CreateBucketResult respCreateBucket =
s3ControlClient.createBucket(reqCreateBucket);
    System.out.printf("CreateBucket Response: %s\n", respCreateBucket.toString());

    return respCreateBucket.getBucketArn();
}
```

Hinzufügen von Tags für S3-on-Outposts-Buckets

Sie können Tags für Ihre Amazon-S3-on-Outposts-Buckets hinzufügen, um die Speicherkosten oder andere Kriterien für einzelne Projekte oder Gruppen von Projekten zu verfolgen.

Note

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der seine Tags ändern kann.

Verwenden der S3-Konsole

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, dessen Tags Sie bearbeiten möchten.
4. Wählen Sie die Registerkarte Eigenschaften aus.
5. Wählen Sie unter Tags, die Option Edit (Bearbeiten) aus.
6. (Optional) Wählen Sie für jede Markierung Add new tag (Neue Markierung hinzufügen) und geben Sie den Schlüsselnamen unter Key (Schlüssel) und den Wert unter Value (Wert) ein.

Fügen Sie alle Tags hinzu, die Sie mit einem Outposts-Bucket verknüpfen möchten, um andere Kriterien für einzelne Projekte oder Gruppen von Projekten zu verfolgen.

7. Wählen Sie Änderungen speichern.

Verwenden Sie den AWS CLI

Im folgenden AWS CLI Beispiel wird eine Tagging-Konfiguration auf einen S3 on Outposts-Bucket angewendet, indem ein JSON Dokument im aktuellen Ordner verwendet wird, das tags () *tagging.json* spezifiziert. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
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"
  }
]
```

Im folgenden AWS CLI Beispiel wird eine Tagging-Konfiguration direkt von der Befehlszeile aus auf einen S3 on Outposts-Bucket angewendet.

```
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}]'
```

Weitere Informationen zu diesem Befehl finden Sie [put-bucket-tagging](#) in der AWS CLI Referenz.

Verwalten des Zugriffs auf einen Amazon-S3-on-Outposts-Bucket mit einer Bucket-Richtlinie

Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) Richtlinie, mit der Sie Zugriffsberechtigungen für Ihren Bucket und die darin enthaltenen Objekte gewähren können. Nur der Bucket-Eigentümer kann einem Bucket eine Richtlinie zuordnen. Die dem Bucket zugeordneten Berechtigungen gelten für alle Objekte im Bucket, die dem Bucket-Eigentümer gehören. Bucket-Richtlinien sind auf eine Größe von 20 KB beschränkt. Weitere Informationen finden Sie unter [Bucket-Richtlinie](#).

Sie können Ihre Bucket-Richtlinie aktualisieren, um den Zugriff auf Ihren Amazon-S3-on-Outposts-Bucket zu verwalten. Weitere Informationen finden Sie unter den folgenden Themen.

Themen

- [Hinzufügen oder Bearbeiten einer Bucket-Richtlinie für einen Amazon-S3-on-Outposts-Bucket](#)
- [Anzeigen der Bucket-Richtlinie für Ihren Amazon-S3-on-Outposts-Bucket](#)
- [Löschen der Bucket-Richtlinie für Ihren Amazon-S3-on-Outposts-Bucket](#)
- [Beispiele für Bucket-Richtlinien](#)

Hinzufügen oder Bearbeiten einer Bucket-Richtlinie für einen Amazon-S3-on-Outposts-Bucket

Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) Richtlinie, mit der Sie Zugriffsberechtigungen für Ihren Bucket und die darin enthaltenen Objekte gewähren können. Nur der Bucket-Eigentümer kann einem Bucket eine Richtlinie zuordnen. Die dem Bucket zugeordneten Berechtigungen gelten für alle Objekte im Bucket, die dem Bucket-Eigentümer gehören. Bucket-Richtlinien sind auf eine Größe von 20 KB beschränkt. Weitere Informationen finden Sie unter [Bucket-Richtlinie](#).

In den folgenden Themen erfahren Sie, wie Sie Ihre Bucket-Richtlinie für Amazon S3 on Outposts mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS SDK for Java aktualisieren.

Verwenden der S3-Konsole

Eine Bucket-Richtlinie erstellen oder bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, dessen Bucket-Richtlinie Sie bearbeiten möchten.
4. Wählen Sie die Registerkarte Berechtigungen.
5. Wählen Sie im Abschnitt Outposts bucket policy (Outposts-Bucket-Richtlinie) die Option Edit (Bearbeiten) aus, um eine neue Richtlinie zu erstellen oder zu bearbeiten.

Sie können nun die S3-on-Outposts-Bucket-Richtlinie hinzufügen oder bearbeiten. Weitere Informationen finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#).

Verwenden Sie den AWS CLI

Im folgenden AWS CLI Beispiel wird eine Richtlinie auf einen Outposts-Bucket angewendet.

1. Speichern Sie die folgende Bucket-Richtlinie in einer JSON Datei. In diesem Beispiel heißt die Datei `policy1.json`. Ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
{
  "Version": "2012-10-17",
```

```

    "Id":"testBucketPolicy",
    "Statement":[
      {
        "Sid":"st1",
        "Effect":"Allow",
        "Principal":{"
          "AWS":"123456789012"
        }},
        "Action":"s3-outposts:*",
        "Resource":"arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket"
      }
    ]
  }

```

2. Reichen Sie die JSON Datei als Teil des `put-bucket-policy` CLI Befehls ein. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

```

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

```

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java legt eine Richtlinie für einen Outposts-Bucket fest.

```

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());
}
```

Anzeigen der Bucket-Richtlinie für Ihren Amazon-S3-on-Outposts-Bucket

Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) Richtlinie, mit der Sie Zugriffsberechtigungen für Ihren Bucket und die darin enthaltenen Objekte gewähren können. Nur der Bucket-Eigentümer kann einem Bucket eine Richtlinie zuordnen. Die dem Bucket zugeordneten Berechtigungen gelten für alle Objekte im Bucket, die dem Bucket-Eigentümer gehören. Bucket-Richtlinien sind auf eine Größe von 20 KB beschränkt. Weitere Informationen finden Sie unter [Bucket-Richtlinie](#).

In den folgenden Themen erfahren Sie, wie Sie Ihre Bucket-Richtlinie für Amazon S3 on Outposts mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS SDK for Java anzeigen können.

Verwenden der S3-Konsole

Eine Bucket-Richtlinie erstellen oder bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, dessen Berechtigung Sie bearbeiten möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus.
5. Im Abschnitt Outposts bucket policy (Outposts-Bucket-Richtlinie) können Sie Ihre vorhandene Bucket-Richtlinie überprüfen. Weitere Informationen finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#).

Verwenden Sie den AWS CLI

Im folgenden AWS CLI Beispiel wird eine Richtlinie für einen Outposts-Bucket abgerufen. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java ruft eine Richtlinie für einen Outposts-Bucket ab.

```
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());  
  
}
```

Löschen der Bucket-Richtlinie für Ihren Amazon-S3-on-Outposts-Bucket

Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) Richtlinie, mit der Sie Zugriffsberechtigungen für Ihren Bucket und die darin enthaltenen Objekte gewähren können. Nur der Bucket-Eigentümer kann einem Bucket eine Richtlinie zuordnen. Die dem Bucket zugeordneten Berechtigungen gelten für alle Objekte im Bucket, die dem Bucket-Eigentümer gehören. Bucket-Richtlinien sind auf eine Größe von 20 KB beschränkt. Weitere Informationen finden Sie unter [Bucket-Richtlinie](#).

In den folgenden Themen erfahren Sie, wie Sie Ihre Bucket-Richtlinie für Amazon S3 on Outposts mithilfe von AWS Management Console oder AWS Command Line Interface (AWS CLI) anzeigen können.

Verwenden der S3-Konsole

Löschen einer Bucket-Richtlinie

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.

2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, dessen Berechtigung Sie bearbeiten möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus.
5. Wählen Sie im Bereich Outposts-Bucket-Richtlinie die Option Löschen aus.
6. Bestätigen Sie das Löschen.

Mit dem AWS CLI

Im folgenden Beispiel wird die Bucket-Richtlinie für einen S3-on-Outposts-Bucket (s3-outposts:DeleteBucket) mithilfe der AWS CLI gelöscht. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Beispiele für Bucket-Richtlinien

Mit den Bucket-Richtlinien von S3 on Outposts können Sie den Zugriff auf Objekte in Ihren S3 on Outposts-Buckets sichern, sodass nur Benutzer mit den entsprechenden Berechtigungen darauf zugreifen können. Sie können sogar verhindern, dass authentifizierte Benutzer ohne die entsprechenden Berechtigungen auf Ihre S3 on Outposts zugreifen.

In diesem Abschnitt werden Beispiele für typische Anwendungsfälle für die Bucket-Richtlinien von S3 on Outposts vorgestellt. Wenn Sie diese Richtlinien testen möchten, ersetzen Sie die *user input placeholders* durch Ihre eigenen Informationen (z. B. Ihren Bucket-Namen).

Um einer Gruppe von Objekten Berechtigungen zu gewähren oder zu verweigern, können Sie Platzhalterzeichen (*) in Amazon-Ressourcennamen (ARNs) und anderen Werten verwenden. Sie können beispielsweise den Zugriff auf Gruppen von Objekten steuern, die mit einem gemeinsamen [Präfix](#) beginnen oder mit einer bestimmten Erweiterung wie `.html` enden.

Weitere Informationen zur Richtliniensprache AWS Identity and Access Management (IAM) finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#).

Note

Beim Testen [s3outposts](#) Wenn Sie die Amazon S3 S3-Konsole verwenden, müssen Sie zusätzliche Berechtigungen erteilen, die für die Konsole erforderlich sind `s3outposts:createendpoints``s3outposts:listendpoints`, z. B., usw.

Zusätzliche Ressourcen für die Erstellung von Bucket-Richtlinien

- Eine Liste der IAM Richtlinienaktionen, Ressourcen und Bedingungsschlüssel, die Sie bei der Erstellung einer Bucket-Richtlinie für S3 on Outposts verwenden können, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 on Outposts](#).
- Anleitungen zur Erstellung Ihrer Richtlinie für S3 on Outposts finden Sie unter [Hinzufügen oder Bearbeiten einer Bucket-Richtlinie für einen Amazon-S3-on-Outposts-Bucket](#).

Themen


- [Verwaltung des Zugriffs auf einen Amazon S3 on Outposts-Bucket auf der Grundlage bestimmter IP-Adressen](#)

Verwaltung des Zugriffs auf einen Amazon S3 on Outposts-Bucket auf der Grundlage bestimmter IP-Adressen

Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) Richtlinie, mit der Sie Zugriffsberechtigungen für Ihren Bucket und die darin enthaltenen Objekte gewähren können. Nur der Bucket-Eigentümer kann einem Bucket eine Richtlinie zuordnen. Die dem Bucket zugeordneten Berechtigungen gelten für alle Objekte im Bucket, die dem Bucket-Eigentümer gehören. Bucket-Richtlinien sind auf eine Größe von 20 KB beschränkt. Weitere Informationen finden Sie unter [Bucket-Richtlinie](#).

Beschränken des Zugriffs auf bestimmte IP-Adressen


Im folgenden Beispiel wird allen Benutzern die Ausführung von [S3 on Outposts-Vorgängen](#) an Objekten in den angegebenen Buckets verweigert, es sei denn, die Anfrage stammt aus dem angegebenen IP-Adressbereich.

 Note

Wenn Sie den Zugriff auf eine bestimmte IP-Adresse einschränken, stellen Sie sicher, dass Sie auch angeben, welche VPC Endpunkte, VPC Quell-IP-Adressen oder externen IP-Adressen auf den S3 on Outposts-Bucket zugreifen können. Andernfalls verlieren Sie möglicherweise den Zugriff auf den Bucket, wenn Ihre Richtlinie allen Benutzern die Ausführung von Buckets verweigert [s3outposts](#) Operationen an Objekten in Ihrem S3 on Outposts-Bucket, ohne dass die entsprechenden Berechtigungen bereits vorhanden sind.

Die Condition Erklärung dieser Richtlinie identifiziert **192.0.2.0/24** als Bereich der zulässigen IP-Adressen der Version 4 (IPv4).

Der Condition Block verwendet die `NotIpAddress` Bedingung und den `aws:SourceIp` Bedingungsschlüssel, bei dem es sich um einen AWS breiten Bedingungsschlüssel handelt. Der `aws:SourceIp`-Bedingungsschlüssel kann nur für öffentliche IP-Adressbereiche verwendet werden. Weitere Informationen zu diesen Bedingungsschlüsseln finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für S3 auf Outposts](#). Die `aws:SourceIp` IPv4 Werte verwenden die CIDR Standardnotation. Weitere Informationen finden Sie in der [Referenz zu den IAM JSON Richtlinienelementen](#) im IAMBenutzerhandbuch.

 Warning

Bevor Sie diese S3 on Outposts verwenden, ersetzen Sie die **192.0.2.0/24** IP-Adressbereich in diesem Beispiel durch einen für Ihren Anwendungsfall geeigneten Wert. Andernfalls verlieren Sie die Möglichkeit, auf Ihren Bucket zuzugreifen.

```
{
  "Version": "2012-10-17",
  "Id": "S3OutpostsPolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3outposts:*",
      "Resource": [
```

```

    "arn:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
accesspoint/EXAMPLE-ACCESS-POINT-NAME"
    "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/DOC-EXAMPLE-BUCKET"
  ],
  "Condition": {
    "NotIpAddress": {
      "aws:SourceIp": "192.0.2.0/24"
    }
  }
}
]
}

```

Erlaube IPv4 sowohl IPv6 Adressen als auch

Wenn Sie anfangen, IPv6 Adressen zu verwenden, empfehlen wir Ihnen, alle Richtlinien Ihrer Organisation mit Ihren IPv6 Adressbereichen zusätzlich zu Ihren bestehenden IPv4 Bereichen zu aktualisieren. Auf diese Weise können Sie sicherstellen, dass die Richtlinien auch bei der Umstellung auf funktionieren IPv6.

Die folgende Beispiel-Bucket-Richtlinie für S3 on Outposts zeigt, wie Sie Bereiche kombinieren IPv4 und IPv6 adressieren können, um alle gültigen IP-Adressen Ihres Unternehmens abzudecken. Die Beispielrichtlinie ermöglicht den Zugriff auf die Beispiel-IP-Adressen **192.0.2.1** und **2001:DB8:1234:5678::1** und verweigert den Zugriff auf die Adressen **203.0.113.1** and **2001::1234:5678::1 DB8 ABCD**.

Der `aws:SourceIp`-Bedingungsschlüssel kann nur für öffentliche IP-Adressbereiche verwendet werden. Die IPv6 Werte für `aws:SourceIp` müssen im Standardformat vorliegen. CIDR Für IPv6 unterstützen wir die Verwendung `::` zur Darstellung eines Bereichs von Nullen (z. B. `2001:DB8:1234:5678::/64`). Weitere Informationen finden Sie im IAM Benutzerhandbuch unter [Operatoren für IP-Adressbedingungen](#).

Warning

Ersetzen Sie die IP-Adressbereiche in diesem Beispiel durch entsprechende Werte für Ihren Anwendungsfall, bevor Sie diese Richtlinie für S3 on Outposts verwenden. Andernfalls verlieren Sie möglicherweise die Möglichkeit, auf Ihren Bucket zuzugreifen.

```

{
  "Id": "S3OutpostsPolicyId2",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIPmix",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3outposts:*",
      "Resource": [
        "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/DOC-EXAMPLE-BUCKET",
        "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-
ID/bucket/DOC-EXAMPLE-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"
          ]
        }
      }
    }
  ]
}

```

Auflisten von Amazon-S3-on-Outposts-Buckets

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine

Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs und Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Weitere Informationen über das Arbeiten mit Buckets in S3 on Outposts finden Sie unter [Arbeiten mit S3-on-Outposts-Buckets](#).

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe von, und eine Liste Ihrer S3-On-Outposts-Buckets zurückgeben können. [AWS Management Console](#) [AWS CLI](#) [AWS SDK for Java](#)

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Sehen Sie sich Ihre Liste der S3-on-Outposts-Buckets unter Outposts buckets (Outposts-Buckets) an.

Mit dem AWS CLI

Im folgenden AWS CLI Beispiel wird eine Liste von Buckets in einem Outpost abgerufen. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen zu diesem Befehl finden Sie [list-regional-buckets](#) in der AWS CLI Referenz.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java ruft eine Liste von Buckets in einem Outpost ab. Weitere Informationen finden Sie [ListRegionalBuckets](#) in der Amazon Simple Storage Service API Reference.

```
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());
}
```

Einen S3 on Outposts Bucket mit dem AWS CLI und dem SDK für Java abrufen

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. VPC Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Die folgenden Beispiele zeigen Ihnen, wie Sie mit dem AWS CLI und AWS SDK for Java einen S3 on Outposts-Bucket abrufen können.

Note

Wenn Sie mit Amazon S3 auf Outposts über das AWS CLI Oder arbeiten AWS SDKs, geben Sie den Access Point ARN für den Outpost anstelle des Bucket-Namens an. Der Access Point ARN hat die folgende Form, wobei der AWS-Region Code für die Region *region* steht, in der sich der Outpost befindet:

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

Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Mit dem AWS CLI

Im folgenden Beispiel wird ein S3-on-Outposts-Bucket mit der AWS CLI abgerufen. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen über diesen Befehl finden Sie unter [get-bucket](#) in der AWS CLI -Referenz.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel für S3 on Outposts ruft einen Bucket mithilfe von SDK for Java ab. Weitere Informationen finden Sie [GetBucket](#) in der Amazon Simple Storage Service API Reference.

```
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());  
  
}
```

Löschen Ihres Amazon-S3-on-Outposts-Buckets

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten

dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Weitere Informationen über das Arbeiten mit Buckets in S3 on Outposts finden Sie unter [Arbeiten mit S3-on-Outposts-Buckets](#).

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der ihn löschen kann.

Note

- Outposts-Buckets müssen leer sein, bevor sie gelöscht werden können.

Die Amazon-S3-Konsole unterstützt keine S3-on-Outposts-Objektaktionen. Um Objekte in einem S3 on Outposts Bucket zu löschen, müssen Sie REST API AWS CLI, oder AWS SDKs verwenden.

- Bevor Sie einen Outposts-Bucket löschen können, müssen Sie alle Outposts-Zugriffspunkte für den Bucket löschen. Weitere Informationen finden Sie unter [Löschen eines Zugriffspunkts](#).
- Sie können einen Bucket nicht wiederherstellen, nachdem er gelöscht wurde.

Die folgenden Beispiele zeigen Ihnen, wie Sie einen S3 on Outposts-Bucket mithilfe von AWS Management Console und AWS Command Line Interface (AWS CLI) löschen.

Verwenden der S3-Konsole

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Bucket, den Sie löschen möchten, und wählen Sie Delete (Löschen).
4. Bestätigen Sie das Löschen.

Verwenden Sie den AWS CLI

Im folgenden Beispiel wird ein S3-on-Outposts-Bucket (s3-outposts:DeleteBucket) mithilfe der AWS CLI gelöscht. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Arbeiten mit Zugriffspunkten von Amazon S3 on Outposts

Um auf Ihren Amazon-S3-on-Outposts-Bucket zuzugreifen, müssen Sie einen Zugriffspunkt erstellen und konfigurieren.

Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in Amazon S3. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind, mit denen Sie Amazon S3-Objekt-Vorgänge ausführen können, z. B. GetObject und PutObject. Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Access Points unterstützen nur virtual-host-style Adressierung.

Note

Derjenige AWS-Konto, der den Outposts-Bucket erstellt, besitzt ihn und ist der einzige, der ihm Access Points zuweisen kann.

In den folgenden Abschnitten wird beschrieben, wie Sie die Zugriffspunkte für S3-on-Outposts-Buckets erstellen und verwalten.

Themen

- [Erstellen eines S3-on-Outposts-Zugriffspunkten](#)
- [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#)
- [Anzeigen von Informationen über eine Zugriffspunktkonfiguration](#)
- [Eine Liste Ihrer Amazon-S3-on-Outposts-Zugriffspunkte anzeigen](#)
- [Löschen eines Zugriffspunkts](#)
- [Hinzufügen oder Bearbeiten einer Zugriffspunktrichtlinie](#)

- [Anzeigen einer Zugriffspunktsrichtlinie für einen S3-on-Outposts-Zugriffspunkt](#)

Erstellen eines S3-on-Outposts-Zugriffspunkten

Um auf Ihren Amazon-S3-on-Outposts-Bucket zuzugreifen, müssen Sie einen Zugriffspunkt erstellen und konfigurieren.

Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in Amazon S3. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind, mit denen Sie Amazon S3-Objekt-Vorgänge ausführen können, z. B. `GetObject` und `PutObject`. Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Access Points unterstützen nur virtual-host-style Adressierung.

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe von, AWS Command Line Interface (AWS CLI) und AWS SDK for Java einen Zugriffspunkt S3 on Outposts erstellen. AWS Management Console

Note

Derjenige AWS-Konto , der den Outposts-Bucket erstellt, besitzt ihn und ist der einzige, der ihm Access Points zuweisen kann.

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, für den Sie einen Outposts-Zugriffspunkt erstellen möchten.
4. Wählen Sie die Registerkarte Outposts-Zugriffspunkte.
5. Wählen Sie im Abschnitt Outposts-Zugriffspunkte die Option Outposts-Zugriffspunkte erstellen aus.
6. Geben Sie in den Einstellungen des Outposts Access Points einen Namen für den Access Point ein und wählen Sie dann die Virtual Private Cloud (VPC) für den Access Point aus.
7. Wenn Sie eine Richtlinie für Ihren Zugriffspunkt hinzufügen möchten, geben Sie sie in den Abschnitt Richtlinien für den Outposts-Zugriffspunkt ein.

Weitere Informationen finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#).

Verwenden Sie den AWS CLI

Example

Im folgenden AWS CLI Beispiel wird ein Access Point für einen Outposts-Bucket erstellt. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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
```

Verwendung des AWS SDK for Java

Example

Das folgende Beispiel SDK für Java erstellt einen Access Point für einen Outposts-Bucket. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

public String createAccessPoint(String bucketArn, String accessPointName) {

    CreateAccessPointRequest reqCreateAP = new CreateAccessPointRequest()
        .withAccountId(AccountId)
        .withBucket(bucketArn)
        .withName(accessPointName)
        .withVpcConfiguration(new VpcConfiguration().withVpcId("vpc-12345"));

    CreateAccessPointResult respCreateAP =
s3ControlClient.createAccessPoint(reqCreateAP);
    System.out.printf("CreateAccessPoint Response: %s\n", respCreateAP.toString());

    return respCreateAP.getAccessPointArn();
}
```

Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets

Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Jedes Mal, wenn Sie einen Zugriffspunkt für einen Bucket erstellen, generiert S3 on Outposts automatisch einen Zugriffspunkt-Alias. Sie können diesen Zugriffspunkt-Alias anstelle eines Zugriffspunkts ARN für jeden Betrieb auf der Datenebene verwenden. Sie können beispielsweise einen Zugriffspunkt-Alias verwenden, um Operationen auf Objektebene wie PUT, GETLIST, und mehr auszuführen. Eine Liste dieser Vorgänge finden Sie unter [Amazon S3 API S3-Operationen zur Verwaltung von Objekten](#).

Die folgenden Beispiele zeigen einen ARN Zugriffspunkt-Alias für einen Access Point mit dem Namen *my-access-point*

- Zugangspunkt ARN — `arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/my-access-point`
- Zugriffspunkt-Alias – `my-access-po-001ac5d28a6a232904e8xz5w8ijx1qzlp3i3kuse10--op-s3`

Weitere Informationen zu finden Sie ARNs unter [Amazon Resource Names \(ARNs\)](#) in der Allgemeine AWS-Referenz.

Weitere Informationen über die Zugriffspunkt-Aliasse finden Sie in den folgenden Themen.

Themen

- [Zugriffspunkt-Aliasse](#)
- [Verwenden eines Zugriffspunkt-Alias in einer Objektoperation von S3 on Outposts](#)
- [Einschränkungen](#)

Zugriffspunkt-Aliasse

Ein Zugriffspunkt-Alias wird innerhalb desselben Namespace wie ein S3-on-Outposts-Bucket erstellt. Wenn Sie einen Zugriffspunkt erstellen, generiert S3 on Outposts automatisch einen Zugriffspunkt-Alias, der nicht geändert werden kann. Ein Zugriffspunkt-Alias erfüllt alle Anforderungen eines gültigen Bucket-Namens von S3 on Outposts und besteht aus den folgenden Teilen:

access point name prefix-metadata--op-s3

Note

Das Suffix `--op-s3` ist für Zugriffspunkt-Alias reserviert. Wir empfehlen, es nicht für Bucket- oder Zugriffspunktnamen zu verwenden. Weitere Informationen zu Bucket-Benennungsregeln für S3 on Outposts finden Sie unter [Arbeiten mit S3-on-Outposts-Buckets](#).

Suchen des Zugriffspunkt-Alias

Die folgenden Beispiele zeigen Ihnen, wie Sie einen Zugriffspunkt-Alias mit der Amazon-S3-Konsole und der AWS CLI finden.

Example : Suchen und Kopieren eines Zugriffspunkt-Alias in der Amazon-S3-Konsole

Nachdem Sie einen Zugriffspunkt in der Konsole erstellt haben, können Sie den Zugriffspunkt-Alias der Spalte Access Point alias (Zugriffspunkt-Alias) der Liste Access Points (Zugriffspunkte) entnehmen.

So kopieren Sie einen Zugriffspunkt-Alias

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts--Zugriffspunkte) aus.
3. Zum Kopieren des Zugriffspunkt-Alias führen Sie einen der folgenden Schritte aus:
 - Wählen Sie in der Liste Access Points (Zugriffspunkte) das Optionsfeld neben dem Namen des Zugriffspunkts und dann Copy Access Point alias (Zugriffspunkt-Alias kopieren) aus.
 - Wählen Sie den Namen des Zugriffspunkts aus. Kopieren Sie dann unter Outposts access point overview (Outposts-Zugriffspunkt – Übersicht) den Zugriffspunkt-Alias.

Example : Erstellen Sie einen Access Point mithilfe von AWS CLI und suchen Sie den Access Point-Alias in der Antwort

Das folgende AWS CLI Beispiel für den `create-access-point` Befehl erstellt den Access Point und gibt den automatisch generierten Access Point-Alias zurück. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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-o01ac5d28a6a232904e8xz5w8ijx1qzlp3i3kuse10--op-s3"
}
```

Example : Rufen Sie einen Zugriffspunkt-Alias ab, indem Sie den AWS CLI

Das folgende AWS CLI Beispiel für den `get-access-point` Befehl gibt Informationen über den angegebenen Zugriffspunkt zurück. Diese Informationen enthalten den Zugriffspunkt-Alias. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

```
{
  "Name": "example-outposts-access-point",
  "Bucket": "example-outposts-bucket",
  "NetworkOrigin": "Vpc",
  "VpcConfiguration": {
    "VpcId": "vpc-01234567890abcdef"
  },
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "IgnorePublicAcls": true,
    "BlockPublicPolicy": true,
    "RestrictPublicBuckets": true
  },
  "CreationDate": "2022-09-18T17:49:15.584000+00:00",
  "Alias": "example-outp-o0b1d075431d83bebde8xz5w8ijx1qzlp3i3kuse10--op-s3"
}
```

Example : Listet Access Points auf, um einen Access Point-Alias zu finden, indem Sie AWS CLI

Das folgende AWS CLI Beispiel für den `list-access-points` Befehl listet Informationen über den angegebenen Access Point auf. Diese Informationen enthalten den Zugriffspunkt-Alias. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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-o0b1d075431d83bebde8xz5w8ijx1qz1bp3i3kuse10--op-s3"
    }
  ]
}
```

Verwenden eines Zugriffspunkt-Alias in einer Objektoperation von S3 on Outposts

Bei der Übernahme von Zugriffspunkten können Sie Zugriffspunkt-Aliasse verwenden, ohne dass umfangreiche Codeänderungen erforderlich sind.

Dieses AWS CLI Beispiel zeigt einen `get-object` Vorgang für einen S3 on Outposts-Bucket. In diesem Beispiel wird `--bucket` anstelle des vollständigen Zugriffspunkts der Alias des Access Points ARN als Wert für verwendet.

```
aws s3api get-object --bucket my-access-po-
o0b1d075431d83bebde8xz5w8ijx1qz1bp3i3kuse10--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": {}
}
```


Einschränkungen

- Aliase können nicht von Kunden konfiguriert werden.
- Aliasse können auf einem Zugriffspunkt nicht gelöscht, geändert oder deaktiviert werden.
- Sie können einen Zugriffspunkt-Alias nicht für Kontrollebenen-Operationen von S3 on Outposts verwenden. Eine Liste von Steuerebenen-Operationen von S3 on Outposts finden Sie unter [Amazon S3 API Control-Operationen für die Verwaltung von Buckets](#).
- Aliase können nicht in Richtlinien AWS Identity and Access Management (IAM) verwendet werden.

Anzeigen von Informationen über eine Zugriffspunktconfiguration

Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in Amazon S3. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind, mit denen Sie Amazon S3-Objekt-Vorgänge ausführen können, z. B. `GetObject` und `PutObject`. Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Access Points unterstützen nur virtual-host-style Adressierung.

In den folgenden Themen erfahren Sie, wie Sie mithilfe von, AWS Command Line Interface (AWS CLI) und AWS SDK for Java Konfigurationsinformationen für einen S3 on AWS Management Console Outposts-Zugriffspunkt zurückgeben.

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts--Zugriffspunkte) aus.
3. Wählen Sie den Outposts-Zugriffspunkt aus, für den Sie Konfigurationsdetails anzeigen möchten.
4. Sehen Sie sich unter Outposts access point overview (Übersicht über Outposts-Zugriffspunkte) die Konfigurationsdetails zum Zugriffspunkt an.

Mit dem AWS CLI

Im folgenden AWS CLI Beispiel wird ein Access Point für einen Outposts-Bucket abgerufen. Ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java ruft einen Access Point für einen Outposts-Bucket ab.

```
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());

}
```

Eine Liste Ihrer Amazon-S3-on-Outposts-Zugriffspunkte anzeigen

Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in Amazon S3. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind, mit denen Sie Amazon S3-Objekt-Vorgänge ausführen können, z. B. `GetObject` und `PutObject`. Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Access Points unterstützen nur virtual-host-style Adressierung.

In den folgenden Themen erfahren Sie, wie Sie mithilfe von, AWS Command Line Interface (AWS CLI) und AWS SDK for Java eine Liste Ihrer S3 on Outposts Access Points zurückgeben können.

AWS Management Console

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts--Zugriffspunkte) aus.
3. Sehen Sie sich Ihre Liste der S3-on-Outposts-Zugriffspunkte unter Outposts access points (Outposts-Zugriffspunkte) an.

Mit dem AWS CLI

Das folgende AWS CLI Beispiel listet die Access Points für einen Outposts-Bucket auf. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java listet die Access Points für einen Outposts-Bucket auf.

```
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());

}
```

Löschen eines Zugriffspunkts

Zugriffspunkte vereinfachen die skalierbare Verwaltung des Datenzugriffs auf freigegebene Datensätze in Amazon S3. Zugriffspunkte sind benannte Netzwerkendpunkte, die Buckets zugeordnet sind, mit denen Sie Amazon S3-Objekt-Vorgänge ausführen können, z. B. `GetObject` und `PutObject`. Bei S3 on Outposts müssen Sie Zugriffspunkte verwenden, um auf ein Objekt in einem Outposts-Bucket zuzugreifen. Access Points unterstützen nur virtual-host-style Adressierung.

Die folgenden Beispiele zeigen Ihnen, wie Sie einen Access Point mithilfe von AWS Management Console und AWS Command Line Interface (AWS CLI) löschen.

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts-Zugriffspunkte) aus.
3. Wählen Sie im Bereich Outposts-Zugriffspunkte den Outposts-Zugriffspunkt aus, den Sie löschen möchten.
4. Wählen Sie Delete (Löschen).
5. Bestätigen Sie das Löschen.

Mit dem AWS CLI

Im folgenden AWS CLI Beispiel wird ein Outposts-Access Point gelöscht. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Hinzufügen oder Bearbeiten einer Zugriffspunktrichtlinie

Jeder Zugriffspunkt verfügt über unterschiedliche Berechtigungen und Netzwerkkontrollen, die Amazon S3 on Outposts auf alle Anforderungen anwendet, die über diesen Zugriffspunkt eingehen. Jeder Zugriffspunkt erzwingt eine benutzerdefinierte Zugriffspunktrichtlinie, die in Verbindung mit der Bucket-Richtlinie funktioniert, die dem zugrunde liegenden Bucket zugeordnet ist. Weitere Informationen finden Sie unter [Zugriffspunkte](#).

In den folgenden Themen erfahren Sie, wie Sie die Zugriffspunktrichtlinie für Ihren S3 on Outposts-Zugriffspunkt mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) und AWS SDK for Java hinzufügen oder bearbeiten.

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, für den Sie die Zugriffspunktrichtlinie bearbeiten möchten.
4. Wählen Sie die Registerkarte Outposts-Zugriffspunkte.
5. Wählen Sie im Abschnitt Outposts-Zugriffspunkte den Zugriffspunkt aus, dessen Richtlinie Sie bearbeiten möchten, und wählen Sie Richtlinie bearbeiten.
6. Fügen Sie die Richtlinie im Abschnitt Richtlinien für den Outposts-Zugriffspunkt hinzu oder bearbeiten Sie sie. Weitere Informationen finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#).

Mit dem AWS CLI

Im folgenden AWS CLI Beispiel wird eine Richtlinie auf einen Outposts-Zugriffspunkt angewendet.

1. Speichern Sie die folgende Zugriffspunktrichtlinie in einer JSON Datei. In diesem Beispiel heißt die Datei `appolicy1.json`. Ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
{
  "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. Reichen Sie die JSON Datei als Teil des `put-access-point-policy` CLI Befehls ein. Ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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
```

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java legt eine Richtlinie für einen Outposts-Zugangspunkt fest.

```
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());
}
```

Anzeigen einer Zugriffspunktrichtlinie für einen S3-on-Outposts-Zugriffspunkt

Jeder Zugriffspunkt verfügt über unterschiedliche Berechtigungen und Netzwerkkontrollen, die Amazon S3 on Outposts auf alle Anforderungen anwendet, die über diesen Zugriffspunkt eingehen. Jeder Zugriffspunkt erzwingt eine benutzerdefinierte Zugriffspunktrichtlinie, die in Verbindung mit der Bucket-Richtlinie funktioniert, die dem zugrunde liegenden Bucket zugeordnet ist. Weitere Informationen finden Sie unter [Zugriffspunkte](#).

Weitere Informationen zum Arbeiten mit Zugriffspunkten in S3 on Outposts finden Sie unter [Arbeiten mit S3-on-Outposts-Buckets](#).

In den folgenden Themen erfahren Sie, wie Sie Ihre Zugriffspunktrichtlinie für S3 on Outposts mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) und AWS SDK for Java anzeigen können.

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts--Zugriffspunkte) aus.
3. Wählen Sie den Outposts-Zugriffspunkt aus, für den Sie die Richtlinie anzeigen möchten.
4. Überprüfen Sie auf dem Tab Permissions (Berechtigungen) die Zugriffspunktrichtlinie für S3 on Outposts.

5. Weitere Informationen zum Bearbeiten der Zugriffspunktrichtlinie finden Sie unter [Hinzufügen oder Bearbeiten einer Zugriffspunktrichtlinie](#).

Mit dem AWS CLI

Im folgenden AWS CLI Beispiel wird eine Richtlinie für einen Outposts-Zugriffspunkt abgerufen. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java ruft eine Richtlinie für einen Outposts-Zugangspunkt ab.

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

public void getAccessPointPolicy(String accessPointArn) {

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

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

}
```

Arbeiten mit Amazon-S3-on-Outposts-Endpunkten

Wenn Sie Anforderungen an einen Zugriffspunkt für Amazon S3 on Outposts weiterleiten möchten, müssen Sie einen S3-on-Outposts-Endpunkt erstellen und konfigurieren. Zum Erstellen eines Endpunkts muss Ihr Service-Link eine aktive Verbindung mit Ihrer Outposts-Heimatregion aufweisen. Jede virtuelle private Cloud (VPC) auf Ihrem Outpost kann einen zugehörigen Endpunkt haben.

Weitere Informationen zu Endpunktkontingenten finden Sie unter [Netzwerkanforderungen von S3 on Outposts](#). Sie müssen einen Endpunkt erstellen, um auf Ihre Outposts-Buckets zugreifen und Objekt-Operationen ausführen zu können. Weitere Informationen finden Sie unter [Endpunkte](#).

Nachdem Sie einen Endpunkt erstellt haben, finden Sie im Feld „Status“ weitere Informationen zum Status des Endpunkts. Wenn deine Outposts offline sind, wird ein CREATE _ FAILED zurückgegeben. Sie können Ihre Service-Link-Verbindung überprüfen, den Endpunkt löschen und das Erstellen erneut versuchen, nachdem die Verbindung wiederhergestellt wurde. Eine Liste mit zusätzlichen Fehlercodes finden Sie nachstehend. Weitere Informationen finden Sie unter [Endpunkte](#).

API	Status	Grund für Fehlschlag – Fehlercode	Meldung – Grund für Fehlschlag
CreateEndpoint	Create_Failed	OutpostNotReachable	Der Endpunkt konnte nicht erstellt werden, da die Service-Link-Verbindung zur Outposts-Heimatregion unterbrochen ist. Überprüfen Sie Ihre Verbindung, löschen Sie den Endpunkt und versuchen Sie es erneut.
CreateEndpoint	Create_Failed	InternalError	Der Endpunkt konnte aufgrund eines internen Fehlers nicht erstellt werden. Bitte löschen Sie den Endpunkt und erstellen Sie ihn erneut.
DeleteEndpoint	Delete_Failed	OutpostNotReachable	Der Endpunkt konnte nicht gelöscht werden, da die Service-Link-Verbindung zur Outposts-Heimatregion unterbrochen ist. Überprüfen Sie Ihre Verbindung und versuchen Sie es erneut.
DeleteEndpoint	Delete_Failed	InternalError	Der Endpunkt konnte aufgrund eines internen Fehlers nicht gelöscht werden. Bitte versuchen Sie es noch einmal.

Weitere Informationen über das Arbeiten mit Buckets in S3 on Outposts finden Sie unter [Arbeiten mit S3-on-Outposts-Buckets](#).

In den folgenden Abschnitten wird die Erstellung und Verwaltung von Endpunkten für S3 on Outposts beschrieben.

Themen

- [Erstellen eines Endpunkts in einem Outpost](#)
- [Anzeigen einer Liste Ihrer Amazon-S3-on-Outposts-Endpunkte](#)
- [Löschen eines Amazon-S3-on-Outposts-Endpunkts](#)

Erstellen eines Endpunkts in einem Outpost

Wenn Sie Anforderungen an einen Zugriffspunkt für Amazon S3 on Outposts weiterleiten möchten, müssen Sie einen S3-on-Outposts-Endpunkt erstellen und konfigurieren. Zum Erstellen eines Endpunkts muss Ihr Service-Link eine aktive Verbindung mit Ihrer Outposts-Heimatregion aufweisen. Jeder virtuellen privaten Cloud (VPC) auf Ihrem Outpost kann ein zugeordneter Endpunkt zugeordnet sein. Weitere Informationen zu Endpunktkontingenten finden Sie unter [Netzwerkanforderungen von S3 on Outposts](#). Sie müssen einen Endpunkt erstellen, um auf Ihre Outposts-Buckets zugreifen und Objekt-Operationen ausführen zu können. Weitere Informationen finden Sie unter [Endpunkte](#).

Berechtigungen

Weitere Informationen zu den erforderlichen Berechtigungen für das Erstellen eines Endpunkts finden Sie unter [Berechtigungen für S3-on-Outposts-Endpunkte](#).

Wenn Sie einen Endpunkt erstellen, erstellt S3 on Outposts auch eine serviceverknüpfte Rolle in Ihrem AWS-Konto. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für S3 on Outposts](#).

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe von, AWS Command Line Interface (AWS CLI) und AWS SDK for Java einen Endpunkt S3 on Outposts erstellen. AWS Management Console

Verwenden der S3-Konsole

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts-Zugriffspunkte) aus.
3. Wählen Sie den Tab Outposts endpoints (Outposts-Endpunkte) aus.
4. Wählen Sie Create Outposts endpoint (Outposts-Endpunkt erstellen) aus.

5. Wählen Sie unter Outpost den Outpost aus, auf dem dieser Endpunkt erstellt werden soll.
6. Wählen Sie unter einen aus VPCVPC, der noch keinen Endpunkt hat und der auch den Regeln für Outposts-Endpunkte entspricht.

Eine virtuelle private Cloud (VPC) ermöglicht es Ihnen, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, kann jedoch die Vorzüge der skalierbaren Infrastruktur von nutze AWS.

Wenn Sie noch keine habenVPC, wählen Sie Create VPC. Weitere Informationen finden Sie unter [Erstellen von Zugriffspunkten, die auf eine virtuelle private Cloud beschränkt sind \(VPC\)](#) im Amazon S3 S3-Benutzerhandbuch.

7. Wählen Sie Create Outposts endpoint (Outposts-Endpunkt erstellen) aus.

Mit dem AWS CLI

Example

Im folgenden AWS CLI Beispiel wird mithilfe des VPC Ressourcenzugriffstyps ein Endpunkt für einen Outpost erstellt. Der VPC wird aus dem Subnetz abgeleitet. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Im folgenden AWS CLI Beispiel wird mithilfe des Zugriffstyps des kundeneigenen IP-Adresspools (CoIP-Pool) ein Endpunkt für einen Outpost erstellt. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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
```

Verwendung des AWS SDK for Java

Example

Das folgende Beispiel SDK für Java erstellt einen Endpunkt für einen Outpost. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.CreateEndpointRequest;
import com.amazonaws.services.s3outposts.model.CreateEndpointResult;

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

    CreateEndpointRequest createEndpointRequest = new CreateEndpointRequest()
        .withOutpostId("op-0d79779cef3c30a40")
        .withSubnetId("subnet-8c7a57c5")
        .withSecurityGroupId("sg-ab19e0d1")
        .withAccessType("CustomerOwnedIp")
        .withCustomerOwnedIpv4Pool("ipv4pool-coip-12345678901234567");
    // Use .withAccessType and .withCustomerOwnedIpv4Pool only when the access type is
    // customer-owned IP address pool (CoIP pool)
    CreateEndpointResult createEndpointResult =
s3OutpostsClient.createEndpoint(createEndpointRequest);
    System.out.println("Endpoint is created and its ARN is " +
createEndpointResult.getEndpointArn());
}
```

Anzeigen einer Liste Ihrer Amazon-S3-on-Outposts-Endpunkte

Wenn Sie Anforderungen an einen Zugriffspunkt für Amazon S3 on Outposts weiterleiten möchten, müssen Sie einen S3-on-Outposts-Endpunkt erstellen und konfigurieren. Zum Erstellen eines Endpunkts muss Ihr Service-Link eine aktive Verbindung mit Ihrer Outposts-Heimatregion aufweisen. Jeder virtuellen privaten Cloud (VPC) auf Ihrem Outpost kann ein zugeordneter Endpunkt zugeordnet sein. Weitere Informationen zu Endpunktkontingenten finden Sie unter [Netzwerkanforderungen von S3 on Outposts](#). Sie müssen einen Endpunkt erstellen, um auf Ihre Outposts-Buckets zugreifen und Objekt-Operationen ausführen zu können. Weitere Informationen finden Sie unter [Endpunkte](#).

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe von, AWS Command Line Interface (AWS CLI) und eine Liste Ihrer S3 on Outposts-Endpunkte zurückgeben können. AWS Management Console
AWS SDK for Java

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts-Zugriffspunkte) aus.

3. Wählen Sie auf der Seite Outposts access points (Outposts-Zugriffspunkte) den Tab Outposts endpoints (Outposts-Endpunkte) aus.
4. Unter Outposts endpoints (Outposts-Endpunkte) können Sie eine Liste Ihrer S3-on-Outposts-Endpunkte anzeigen.

Mit dem AWS CLI

Das folgende AWS CLI Beispiel listet die Endpunkte für die AWS Outposts Ressourcen auf, die Ihrem Konto zugeordnet sind. Weitere Informationen über diesen Befehl finden Sie unter [list-endpoints](#) in der AWS CLI -Referenz.

```
aws s3outposts list-endpoints
```

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java listet die Endpunkte für einen Outpost auf. Weitere Informationen finden Sie [ListEndpoints](#) in der Amazon Simple Storage Service API Reference.

```
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);
}
```

Löschen eines Amazon-S3-on-Outposts-Endpunkts

Wenn Sie Anforderungen an einen Zugriffspunkt für Amazon S3 on Outposts weiterleiten möchten, müssen Sie einen S3-on-Outposts-Endpunkt erstellen und konfigurieren. Zum Erstellen eines Endpunkts muss Ihr Service-Link eine aktive Verbindung mit Ihrer Outposts-Heimatregion aufweisen. Jeder virtuellen privaten Cloud (VPC) auf Ihrem Outpost kann ein Endpunkt zugeordnet sein.

Weitere Informationen zu Endpunktkontingenten finden Sie unter [Netzwerkanforderungen von S3 on Outposts](#). Sie müssen einen Endpunkt erstellen, um auf Ihre Outposts-Buckets zugreifen und Objekt-Operationen ausführen zu können. Weitere Informationen finden Sie unter [Endpunkte](#).

Die folgenden Beispiele zeigen Ihnen, wie Sie Ihre S3 on Outposts-Endpunkte mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) und löschen. AWS SDK for Java

Verwenden der S3-Konsole

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts access points (Outposts-Zugriffspunkte) aus.
3. Wählen Sie auf der Seite Outposts access points (Outposts-Zugriffspunkte) den Tab Outposts endpoints (Outposts-Endpunkte) aus.
4. Wählen Sie unter Outposts endpoints (Outposts-Endpunkte) den Endpunkt aus, den Sie löschen möchten, und klicken Sie dann auf Delete (Löschen).

Mit dem AWS CLI

Das folgende AWS CLI Beispiel löscht einen Endpunkt für einen Outpost. Zum Ausführen dieses Befehls ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel SDK für Java löscht einen Endpunkt für einen Outpost. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
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.");
}
```

Arbeiten mit S3-on-Outposts-Objekten

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. VPC Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden.

Objekte sind die Grundeinheiten, die in Amazon S3 on Outposts gespeichert sind. Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point Amazon Resource Name (ARN) oder den Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Zugriffspunkten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, die ID, die AWS-Konto Outpost-ID und den Namen des Access Points enthält:

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

Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Das Objekt ARNs verwendet das folgende Format, das die Adresse, auf AWS-Region die sich der Outpost bezieht, die ID, die AWS-Konto Outpost-ID, den Bucket-Namen und den Objektschlüssel umfasst:

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

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie ein AWS Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Themen

- [Laden Sie ein Objekt in einen S3-Bucket auf Outposts hoch](#)
- [Kopieren eines Objekts in einem Amazon S3 on Outposts-Bucket mit dem AWS SDK for Java](#)
- [Abrufen eines Objekts aus einem Amazon-S3-on-Outposts-Bucket](#)
- [Auflisten der Objekten in einem Amazon-S3-on-Outposts-Bucket](#)
- [Löschen von Objekten in Amazon-S3-on-Outposts-Buckets](#)
- [Wird verwendet HeadBucket , um festzustellen, ob ein S3 on Outposts-Bucket existiert und Sie über Zugriffsberechtigungen verfügen](#)
- [Durchführen und Verwalten eines mehrteiligen Uploads mit dem SDK für Java](#)
- [Presigned URLs for S3 auf Outposts verwenden](#)
- [Amazon S3 auf Outposts mit lokalem Amazon EMR on Outposts](#)
- [Autorisierungs- und Authentifizierungs-Caching](#)

Laden Sie ein Objekt in einen S3-Bucket auf Outposts hoch

Objekte sind die Grundeinheiten, die in Amazon S3 on Outposts gespeichert sind. Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point Amazon Resource Name (ARN) oder den Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Zugriffspunkten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, die ID, die AWS-Konto Outpost-ID und den Namen des Access Points enthält:

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


Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie AWS ein Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Im Folgenden AWS CLI und in AWS SDK for Java Beispielen wird gezeigt, wie Sie mithilfe eines Access Points ein Objekt in einen S3 on Outposts-Bucket hochladen.

AWS CLI

Example

Im folgenden Beispiel wird ein Objekt mit dem Namen `sample-object.xml` in einen S3-on-Outposts-Bucket (`s3-outposts:PutObject`) mit der AWS CLI eingefügt. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen über diesen Befehl finden Sie unter [put-object](#) in der AWS CLI -Referenz.

```
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

Im folgenden Beispiel wird ein Objekt mithilfe von SDK for Java in einen S3-Bucket auf Outposts eingefügt. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
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.ObjectMetadata;  
import com.amazonaws.services.s3.model.PutObjectRequest;
```

```
import java.io.File;

public class PutObject {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String stringObjKeyName = "*** String object key name ***";
        String fileObjKeyName = "*** File object key name ***";
        String fileName = "*** Path to file to upload ***";

        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 a text string as a new object.
            s3Client.putObject(accessPointArn, stringObjKeyName, "Uploaded String
Object");

            // Upload a file as a new object with ContentType and title specified.
            PutObjectRequest request = new PutObjectRequest(accessPointArn,
fileObjKeyName, new File(fileName));
            ObjectMetadata metadata = new ObjectMetadata();
            metadata.setContentType("plain/text");
            metadata.addUserMetadata("title", "someTitle");
            request.setMetadata(metadata);
            s3Client.putObject(request);
        } 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();
        }
    }
}
```

Kopieren eines Objekts in einem Amazon S3 on Outposts-Bucket mit dem AWS SDK for Java

Objekte sind die Grundeinheiten, die in Amazon S3 on Outposts gespeichert sind. Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point Amazon Resource Name (ARN) oder den Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Zugriffspunkten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, die ID, die AWS-Konto Outpost-ID und den Namen des Access Points enthält:

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

Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie AWS ein Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Das folgenden Beispiel veranschaulicht, wie Sie mithilfe von AWS SDK for Java ein Objekt in einem S3-on-Outposts-Bucket kopieren.

Verwendung des AWS SDK for Java

Das folgende Beispiel für S3 on Outposts kopiert ein Objekt mithilfe von SDK for Java in ein neues Objekt im selben Bucket. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

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

Abrufen eines Objekts aus einem Amazon-S3-on-Outposts-Bucket

Objekte sind die Grundeinheiten, die in Amazon S3 on Outposts gespeichert sind. Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point Amazon Resource Name (ARN) oder den Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Zugriffspunkten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, die ID, die AWS-Konto Outpost-ID und den Namen des Access Points enthält:

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

Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie AWS ein Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Die folgenden Beispiele veranschaulichen, wie Sie ein Objekt mithilfe der AWS Command Line Interface (AWS CLI) und AWS SDK for Java herunterladen (abrufen).

Mit dem AWS CLI

Im folgenden Beispiel wird ein Objekt mit dem Namen `sample-object.xml` in einem S3-on-Outposts-Bucket (`s3-outposts:GetObject`) mit der AWS CLI abgerufen. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen über diesen Befehl finden Sie unter [get-object](#) in der AWS CLI -Referenz.

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

Verwendung des AWS SDK for Java

Das folgende Beispiel für S3 on Outposts ruft ein Objekt mithilfe von SDK for Java ab. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen. Weitere Informationen finden Sie [GetObject](#) in der Amazon Simple Storage Service API Reference.

```
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;
```

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

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;

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

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

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

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

            // Get an entire object, overriding the specified response headers, and
            print the object's content.
            ResponseHeaderOverrides headerOverrides = new ResponseHeaderOverrides()
```

```
        .withCacheControl("No-cache")
        .withContentDisposition("attachment; filename=example.txt");
    GetObjectRequest getObjectRequestHeaderOverride = new
GetObjectRequest(accessPointArn, key)
        .withResponseHeaders(headerOverrides);
    headerOverrideObject = s3Client.getObject(getObjectRequestHeaderOverride);
    displayTextInputStream(headerOverrideObject.getObjectContent());
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it, so it returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
} finally {
    // To ensure that the network connection doesn't remain open, close any
open input streams.
    if (fullObject != null) {
        fullObject.close();
    }
    if (objectPortion != null) {
        objectPortion.close();
    }
    if (headerOverrideObject != null) {
        headerOverrideObject.close();
    }
}
}

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

Auflisten der Objekten in einem Amazon-S3-on-Outposts-Bucket

Objekte sind die Grundeinheiten, die in Amazon S3 on Outposts gespeichert sind. Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point Amazon Resource Name (ARN) oder den Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Zugriffspunkten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, die ID, die AWS-Konto Outpost-ID und den Namen des Access Points enthält:

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

Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Note

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie AWS ein Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Die folgenden Beispiele zeigen Ihnen, wie Sie die Objekte in einem S3-Bucket auf Outposts mithilfe von AWS CLI und AWS SDK for Java auflisten.

Mit dem AWS CLI

Im folgenden Beispiel werden die Objekte in einem S3-on-Outposts-Bucket (`s3-outposts:ListObjectsV2`) unter Verwendung der AWS CLI aufgelistet. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen zu diesem Befehl finden Sie unter [list-objects-v2](#) in der AWS CLI Referenz.


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

Note

Wenn Sie diese Aktion mit Amazon S3 auf Outposts über die verwenden AWS SDKs, geben Sie den Outposts-Access Point ARN anstelle des Bucket-Namens in der folgenden Form an: `arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-Outposts-Access-Point` Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Verwendung des AWS SDK for Java

Das folgende Beispiel für S3 on Outposts listet Objekte in einem Bucket unter Verwendung von SDK for Java auf. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

⚠ Important

In diesem Beispiel wird [ListObjectsV2](#) verwendet, die neueste Version der ListObjects API Operation. Wir empfehlen, diesen überarbeiteten API Vorgang für die Anwendungsentwicklung zu verwenden. Aus Gründen der Abwärtskompatibilität unterstützt Amazon S3 weiterhin die vorherige Version dieses API Vorgangs.

```
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();
}
}
```

Löschen von Objekten in Amazon-S3-on-Outposts-Buckets

Objekte sind die Grundeinheiten, die in Amazon S3 on Outposts gespeichert sind. Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point Amazon Resource Name (ARN) oder den Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Zugriffspunkten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, die ID, die AWS-Konto Outpost-ID und den Namen des Access Points enthält:

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

Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie AWS ein Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Die folgenden Beispiele zeigen Ihnen, wie Sie ein einzelnes Objekt oder mehrere Objekte in einem S3-Bucket auf Outposts mithilfe von AWS Command Line Interface (AWS CLI) und AWS SDK for Java löschen.

Mit dem AWS CLI

Die folgenden Beispiele veranschaulichen, wie Sie ein einzelnes Objekt oder mehrere Objekte aus einem S3-on-Outposts-Bucket löschen.

delete-object

Im folgenden Beispiel wird ein Objekt mit dem Namen `sample-object.xml` in einem S3-on-Outposts-Bucket (`s3-outposts:DeleteObject`) mithilfe der AWS CLI gelöscht. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen über diesen Befehl finden Sie unter [delete-object](#) in der AWS CLI -Befehlsreferenz.

```
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

Im folgenden Beispiel werden zwei Objekte mit dem Namen `sample-object.xml` und `test1.txt` in einem S3-on-Outposts-Bucket (`s3-outposts:DeleteObject`) mithilfe der AWS CLI gelöscht. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen zu diesem Befehl finden Sie unter [delete-objects](#) in der AWS CLI -Referenz.

```
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
}
```

Verwendung des AWS SDK for Java

Die folgenden Beispiele veranschaulichen, wie Sie ein einzelnes Objekt oder mehrere Objekte aus einem S3-on-Outposts-Bucket löschen.

DeleteObject

Das folgende Beispiel für S3 on Outposts löscht ein Objekt in einem Bucket mithilfe von SDK for Java. Um dieses Beispiel zu verwenden, geben Sie den Zugriffspunkt ARN für den Outpost und den Schlüsselnamen für das Objekt an, das Sie löschen möchten. Weitere Informationen finden Sie [DeleteObject](#) in der Amazon Simple Storage Service API Reference.

```
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

Das folgende Beispiel für S3 on Outposts lädt Objekte in einem Bucket hoch und löscht sie dann mithilfe von for Java. SDK Um dieses Beispiel zu verwenden, geben Sie den Zugriffspunkt ARN für den Outpost an. Weitere Informationen finden Sie [DeleteObjects](#) in der Amazon Simple Storage Service API Reference.

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

Wird verwendet HeadBucket , um festzustellen, ob ein S3 on Outposts-Bucket existiert und Sie über Zugriffsberechtigungen verfügen

Objekte sind die Grundeinheiten, die in Amazon S3 on Outposts gespeichert sind. Jedes Objekt ist in einem Bucket enthalten. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket zuzugreifen. Wenn Sie den Bucket für Objektoperationen angeben, verwenden Sie den Access Point Amazon Resource Name (ARN) oder den Access Point-Alias. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Das folgende Beispiel zeigt das ARN Format für S3 auf Outposts-Zugriffspunkten, das den AWS-Region Code für die Region, in der der Outpost beheimatet ist, die ID, die AWS-Konto Outpost-ID und den Namen des Access Points enthält:

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

Weitere Informationen zu S3 on Outposts finden Sie ARNs unter [Ressource ARNs für S3 auf Outposts](#).

Note

Mit Amazon S3 on Outposts werden Objektdaten immer im Outpost gespeichert. Wenn Sie AWS ein Outpost-Rack installieren, bleiben Ihre Daten lokal in Ihrem Outpost, um die Anforderungen an die Datenresidenz zu erfüllen. Ihre Objekte verlassen niemals Ihren Outpost und befinden sich nicht in einer AWS-Region. Da das in der Region gehostet AWS Management Console wird, können Sie die Konsole nicht zum Hochladen oder Verwalten von Objekten in Ihrem Outpost verwenden. Sie können jedoch das, AWS Command Line Interface (AWS CLI) und verwenden RESTAPI, AWS SDKs um Ihre Objekte über Ihre Access Points hochzuladen und zu verwalten.

Die folgenden AWS Command Line Interface (AWS CLI) und AWS SDK for Java Beispiele zeigen Ihnen, wie Sie mithilfe des HeadBucket API Vorgangs ermitteln können, ob ein Amazon S3 on Outposts-Bucket vorhanden ist und ob Sie die Berechtigung haben, darauf zuzugreifen. Weitere Informationen finden Sie [HeadBucket](#) in der Amazon Simple Storage Service API Reference.

Mit dem AWS CLI

Das folgende AWS CLI Beispiel für S3 on Outposts verwendet den `head-bucket` Befehl, um festzustellen, ob ein Bucket vorhanden ist und Sie über Zugriffsberechtigungen verfügen. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen über diesen Befehl finden Sie unter [head-bucket](#) in der AWS CLI -Referenz.

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


Verwendung des AWS SDK for Java

Das folgende S3-on-Outposts-Beispiel veranschaulicht, wie Sie feststellen, ob ein Bucket vorhanden ist und ob Sie Zugriffsberechtigungen für diesen Bucket besitzen. Um dieses Beispiel zu verwenden, geben Sie den Zugriffspunkt ARN für den Outpost an. Weitere Informationen finden Sie [HeadBucket](#) in der Amazon Simple Storage Service API Reference.

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

Durchführen und Verwalten eines mehrteiligen Uploads mit dem SDK für Java

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts Ressourcen erstellen und Objekte vor Ort für Anwendungen speichern und abrufen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Die folgenden Beispiele zeigen, wie Sie S3 auf Outposts verwenden können, AWS SDK for Java um einen mehrteiligen Upload durchzuführen und zu verwalten.

Themen

- [Durchführen eines mehrteiligen Uploads eines Objekts in einem S3-on-Outposts-Bucket](#)
- [Kopieren eines großen Objekts in einem S3-on-Outposts-Bucket mithilfe eines mehrteiligen Uploads](#)
- [Auflisten von Teilen eines Objekts in einem S3-on-Outposts-Bucket](#)
- [Abrufen einer Liste der in Bearbeitung befindlichen mehrteiligen Uploads in einem S3-on-Outposts-Bucket](#)

Durchführen eines mehrteiligen Uploads eines Objekts in einem S3-on-Outposts-Bucket

Das folgende Beispiel für S3 on Outposts initiiert, lädt und beendet einen mehrteiligen Upload eines Objekts in einen Bucket mithilfe von for Java. SDK Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen. Weitere Informationen finden Sie unter [Hochladen eines Objekts mithilfe eines mehrteiligen Uploads](#) im Amazon Simple Storage Service-Benutzerhandbuch.

```
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;
}
```

Kopieren eines großen Objekts in einem S3-on-Outposts-Bucket mithilfe eines mehrteiligen Uploads

Das folgende Beispiel für S3 on Outposts verwendet SDK for Java, um ein Objekt in einen Bucket zu kopieren. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
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;
    }
}

```

Auflisten von Teilen eines Objekts in einem S3-on-Outposts-Bucket

Das folgende Beispiel für S3 on Outposts listet die Teile eines Objekts in einem Bucket unter Verwendung von SDK for Java auf. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```

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();
}
}
```

Abrufen einer Liste der in Bearbeitung befindlichen mehrteiligen Uploads in einem S3-on-Outposts-Bucket

Das folgende Beispiel für S3 on Outposts zeigt, wie Sie mithilfe von Java eine Liste der laufenden mehrteiligen Uploads aus einem Outposts-Bucket abrufen. SDK Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
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();
}
}
```

Presigned URLs for S3 auf Outposts verwenden

Um zeitlich begrenzten Zugriff auf Objekte zu gewähren, die lokal in einem Outpost gespeichert sind, ohne Ihre Bucket-Richtlinie zu aktualisieren, können Sie eine vorsignierte Version verwenden. URL Mit der Option vorsigniert URLs können Sie als Bucket-Besitzer Objekte mit Personen in Ihrer virtuellen privaten Cloud (VPC) teilen oder ihnen die Möglichkeit geben, Objekte hochzuladen oder zu löschen.

Wenn Sie ein vorsigniertes Objekt mithilfe URL von AWS SDKs oder AWS Command Line Interface (AWS CLI) erstellen, verknüpfen Sie es URL mit einer bestimmten Aktion. Sie gewähren auch zeitlich begrenzten Zugriff auf die vorsignierte Datei, URL indem Sie eine benutzerdefinierte Ablaufzeit wählen, die so niedrig wie 1 Sekunde und maximal 7 Tage sein kann. Wenn Sie den Vorsignierten teilenURL, VPC kann die Person in der die Aktion so ausführen, URL als wäre sie der ursprüngliche signierende Benutzer. Wenn der seine Ablaufzeit URL erreicht hat, URL läuft der ab und funktioniert nicht mehr.

Einschränkung vordefinierter Funktionen URL

Die Funktionen einer vorsignierten Datei URL werden durch die Berechtigungen des Benutzers begrenzt, der sie erstellt hat. Im Wesentlichen URLs handelt es sich bei vorsignierten Token um Inhaber-Token, die denjenigen Zugriff gewähren, die sie besitzen. Daher empfehlen wir Ihnen, sie angemessen zu schützen.

AWS Signatur Version 4 (SigV4)

Um ein bestimmtes Verhalten bei der Authentifizierung vorsignierter URL Anfragen mithilfe von AWS Signature Version 4 (Sigv4) durchzusetzen, können Sie Bedingungsschlüssel in Bucket-Richtlinien und Access-Point-Richtlinien verwenden. Sie können beispielsweise eine Bucket-Richtlinie erstellen, die die `s3-outposts:signatureAge` Bedingung verwendet, um alle vorsignierten Amazon S3 on URL Outposts-Anfragen für Objekte im `example-outpost-bucket` Bucket abzulehnen, wenn die Signatur älter als 10 Minuten ist. Um dieses Beispiel zu verwenden, ersetzen Sie *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Deny a presigned URL request if the signature is more than 10
minutes old",
      "Effect": "Deny",
      "Principal": {"AWS": "444455556666"},
      "Action": "s3-outposts:*",
      "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/object/
*",
      "Condition": {
        "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
        "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
      }
    }
  ]
}
```

```
}  
  }  
] }  
}
```

Eine Liste von Bedingungsschlüsseln und zusätzliche Beispielrichtlinien, mit denen Sie ein bestimmtes Verhalten bei der Authentifizierung von vorab signierten URL Anfragen mithilfe von Signature Version 4 erzwingen können, finden Sie unter. [AWS Authentifizierungsspezifische Richtlinien](#)
[Richtlinienschlüssel für Signature Version 4 \(Sigv4\)](#)

Beschränkung der Netzwege

Wenn Sie die Verwendung von vorsignierten URLs und allen S3-On-Outposts-Zugriffen auf bestimmte Netzwerkpfade einschränken möchten, können Sie Richtlinien schreiben, die einen bestimmten Netzwerkpfad erfordern. Um die Beschränkung für den IAM Prinzipal festzulegen, der den Anruf tätigt, können Sie identitätsbasierte AWS Identity and Access Management (IAM) Richtlinien verwenden (z. B. Benutzer-, Gruppen- oder Rollenrichtlinien). Um die Beschränkung für die Ressource S3 on Outposts festzulegen, können Sie ressourcenbasierte Richtlinien verwenden (z. B. Bucket- und Zugriffspunkt-Richtlinien).

Eine Netzwerkpfadbeschränkung für den IAM Prinzipal erfordert, dass der Benutzer mit diesen Anmeldeinformationen Anfragen vom angegebenen Netzwerk aus stellt. Eine Einschränkung des Buckets oder des Zugriffspunkts erfordert, dass alle Anfragen an diese Ressource aus dem angegebenen Netz stammen. Diese Einschränkungen gelten auch außerhalb des URL vordefinierten Szenarios.

Welche IAM globale Bedingung Sie verwenden, hängt vom Typ des Endpunkts ab. Wenn Sie den öffentlichen Endpunkt für S3 on Outposts verwenden, benutzen Sie `aws:SourceIp`. Wenn Sie einen VPC Endpunkt für S3 auf Outposts verwenden, verwenden Sie `aws:SourceVpc` oder `aws:SourceVpce`.

Die folgende IAM Richtlinienerklärung verlangt, dass der Principal AWS nur über den angegebenen Netzwerkbereich zugreift. Mit dieser Richtlinie müssen alle Zugriffe von diesem Bereich ausgehen. Dies gilt auch für den Fall, dass jemand ein URL für S3 vorsigniertes Gerät auf Outposts verwendet. Um dieses Beispiel zu verwenden, ersetzen Sie *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen.

```
{  
  "Sid": "NetworkRestrictionForIAMPrincipal",  
  "Effect": "Deny",
```

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

Ein Beispiel für eine Bucket-Richtlinie, die den `aws:SourceIP` AWS globalen Bedingungsschlüssel verwendet, um den Zugriff auf einen S3 on Outposts-Bucket auf einen bestimmten Netzwerkbereich zu beschränken, finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#).

Wer kann einen vorsignierten erstellen URL

Jeder, der über gültige Sicherheitsanmeldedaten verfügt, kann eine URL vorsignierte erstellen. Damit ein Benutzer jedoch erfolgreich auf ein Objekt zugreifen kann, URL muss das vorsignierte Objekt von einer Person erstellt worden sein, die berechtigt URL ist, den Vorgang auszuführen, auf dem das vorsignierte Objekt basiert. VPC

Sie können die folgenden Anmeldeinformationen verwenden, um ein vorsigniertes Objekt zu erstellen: URL

- IAMInstanzprofil — Gültig bis zu 6 Stunden.
- AWS Security Token Service— Gültig bis zu 36 Stunden, wenn es mit dauerhaften Anmeldeinformationen signiert ist, z. B. den Anmeldeinformationen des AWS-Konto Root-Benutzers oder eines IAM Benutzers.
- IAMBenutzer — Gültig bis zu 7 Tage, wenn Sie AWS Signature Version 4 verwenden.

Um eine vorsignierte Version zu erstellenURL, die bis zu 7 Tage gültig ist, delegieren Sie zunächst die IAM Benutzeranmeldedaten (den Zugriffsschlüssel und den geheimen Schlüssel) an dieSDK, die Sie verwenden. Generieren Sie dann mithilfe URL von AWS Signature Version 4 eine vorsignierte.

Note

- Wenn Sie ein vorsigniertes URL mithilfe eines temporären Tokens erstellt haben, URL läuft das ab, wenn das Token abläuft, auch wenn Sie das URL mit einer späteren Ablaufzeit erstellt haben.

- Da vorab signierte URLs Personen Zugriff auf Ihre S3 on Outposts-Buckets gewähren, empfehlen wir Ihnen URL, diese entsprechend zu schützen. Weitere Informationen zum Schutz URLs vorsignierter Benutzer finden Sie unter. [Einschränkung vordefinierter Funktionen URL](#)

Wann überprüft S3 on Outposts das Ablaufdatum und die Uhrzeit eines vorab URL signierten?

Zum Zeitpunkt der HTTP Anfrage überprüft S3 on Outposts das Ablaufdatum und die Uhrzeit einer signierten URL Nachricht. Beginnt ein Client beispielsweise mit dem Herunterladen einer großen Datei unmittelbar vor der Ablaufzeit, wird der Download auch dann fortgesetzt, wenn die Ablaufzeit während des Downloads verstreicht. Wenn die Verbindung jedoch unterbrochen wird und der Client versucht, den Download nach Ablauf der Zeit erneut zu starten, schlägt der Download fehl.

Weitere Informationen zur Verwendung eines Presigned URL zum Teilen oder Hochladen von Objekten finden Sie in den folgenden Themen.

Themen

- [Objekte mithilfe von Presigned teilen URLs](#)
- [Generieren eines VorsigniertenURL, um ein Objekt in einen S3 on Outposts-Bucket hochzuladen](#)

Objekte mithilfe von Presigned teilen URLs

Um zeitlich begrenzten Zugriff auf Objekte zu gewähren, die lokal in einem Outpost gespeichert sind, ohne Ihre Bucket-Richtlinie zu aktualisieren, können Sie ein vorsigniertes Objekt verwenden. URL Mit der Option vorsigniert URLs können Sie als Bucket-Besitzer Objekte mit Personen in Ihrer virtuellen privaten Cloud (VPC) teilen oder ihnen die Möglichkeit geben, Objekte hochzuladen oder zu löschen.

Wenn Sie ein vorsigniertes Objekt mithilfe URL von AWS SDKs oder AWS Command Line Interface (AWS CLI) erstellen, verknüpfen Sie es URL mit einer bestimmten Aktion. Sie gewähren auch zeitlich begrenzten Zugriff auf die vorsignierte Datei, URL indem Sie eine benutzerdefinierte Ablaufzeit wählen, die so niedrig wie 1 Sekunde und maximal 7 Tage sein kann. Wenn Sie den Vorsignierten teilenURL, VPC kann die Person in der die Aktion so ausführen, URL als wäre sie der ursprüngliche signierende Benutzer. Wenn der seine Ablaufzeit URL erreicht hat, URL läuft der ab und funktioniert nicht mehr.

Wenn Sie eine vorsignierte Datei erstellen URL, müssen Sie Ihre Sicherheitsanmeldedaten und anschließend Folgendes angeben:

- Ein Access Point Amazon Resource Name (ARN) für den Amazon S3 on Outposts-Bucket
- Ein Objektschlüssel
- Eine HTTP Methode (GET zum Herunterladen von Objekten)
- Ein Verfallsdatum und eine Verfallszeit

Ein vorsignierter URL Code ist nur für die angegebene Dauer gültig. Das heißt, Sie müssen die Aktion starten, die bis zum Datum und zur Uhrzeit URL vor dem Ablaufdatum zulässig ist. Sie können eine vorsignierte Option URL mehrfach verwenden, bis das Ablaufdatum und die Ablaufzeit erreicht sind. Wenn Sie ein vorsigniertes Token URL mithilfe eines temporären Tokens erstellt haben, URL läuft das ab, wenn das Token abläuft, auch wenn Sie das URL mit einer späteren Ablaufzeit erstellt haben.

Benutzer in der Virtual Private Cloud (VPC), die Zugriff auf das vorsignierte Objekt haben, URL können auf das Objekt zugreifen. Wenn Sie beispielsweise ein Video in Ihrem Bucket haben und sowohl der Bucket als auch das Objekt privat sind, können Sie das Video mit anderen teilen, indem Sie ein URL vorsigniertes Video generieren. Da vorab signierte URLs Personen Zugriff auf Ihre S3 on Outposts-Buckets gewähren, empfehlen wir Ihnen URL, diese entsprechend zu schützen. URLs Weitere Informationen zum Schutz URLs vorsignierter Benutzer finden Sie unter. [Einschränkung vordefinierter Funktionen URL](#)

Jeder, der über gültige Sicherheitsanmeldedaten verfügt, kann eine URL vorsignierte erstellen. Das Vorsignierte URL muss jedoch von einer Person erstellt werden, die berechtigt ist, den Vorgang auszuführen, auf dem das Vorsignierte URL basiert. Weitere Informationen finden Sie unter [Wer kann einen vorsignierten erstellen URL](#).

Sie können ein vorsigniertes Objekt für URL die gemeinsame Nutzung eines Objekts in einem S3-Bucket auf Outposts generieren, indem Sie den AWS SDKs und den verwenden. AWS CLI Weitere Informationen finden Sie in den folgenden Beispielen.

Mit dem AWS SDKs

Sie können das verwenden AWS SDKs, um ein vorsigniertes Objekt zu generieren URL, das Sie an andere weitergeben können, damit diese ein Objekt abrufen können.

Note

Wenn Sie das verwenden, AWS SDKs um ein vorsigniertes Objekt zu generierenURL, beträgt die maximale Ablaufzeit für ein vorsigniertes Objekt URL 7 Tage ab dem Zeitpunkt der Erstellung.

Java

Example

Im folgenden Beispiel wird ein vorsigniertes Objekt generiertURL, das Sie an andere weitergeben können, damit diese ein Objekt aus einem S3-Bucket auf Outposts abrufen können. Weitere Informationen finden Sie unter [Presigned URLs for S3 auf Outposts verwenden](#). Um dieses Beispiel zu verwenden, ersetzen Sie *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen.

```
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

Im folgenden Beispiel wird ein vorsigniertes Objekt generiertURL, das Sie an andere weitergeben können, damit diese ein Objekt aus einem S3-Bucket auf Outposts abrufen können. Weitere Informationen finden Sie unter [Presigned URLs for S3 auf Outposts verwenden](#). Um dieses Beispiel zu verwenden, ersetzen Sie *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen.

```
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

Im folgenden Beispiel wird mithilfe von SDK for Python (Boto3) ein für die gemeinsame Nutzung eines Objekts vorsigniertes URL Objekt generiert. Verwenden Sie beispielsweise einen Boto3-Client und die `generate_presigned_url` Funktion, um einen vorsignierten Client zu generieren, mit dem Sie ein Objekt URL erstellen können. GET

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

Weitere Informationen zur Verwendung von SDK for Python (Boto3) zum Generieren eines Vorsignierten URL finden Sie unter [Python in der Referenz](#). AWS SDK for Python (Boto) API

Verwenden von AWS CLI

Der folgende AWS CLI Beispielbefehl generiert einen URL für einen S3 on Outposts-Bucket vorsignierten Bucket. Um dieses Beispiel zu verwenden, ersetzen Sie den *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen.

Note

Wenn Sie das verwenden, AWS CLI um ein vorsigniertes zu generieren URL, beträgt die maximale Ablaufzeit für ein vorsigniertes URL Dokument 7 Tage ab dem Zeitpunkt der Erstellung.

```
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
```

Weitere Informationen finden Sie unter [vorsignieren](#) in der AWS CLI Befehlsreferenz.

Generieren eines VorsigniertenURL, um ein Objekt in einen S3 on Outposts-Bucket hochzuladen

Um zeitlich begrenzten Zugriff auf Objekte zu gewähren, die lokal in einem Outpost gespeichert sind, ohne Ihre Bucket-Richtlinie zu aktualisieren, können Sie ein vorsigniertes Objekt verwenden. URL Mit der Option vorsigniert URLs können Sie als Bucket-Besitzer Objekte mit Personen in Ihrer virtuellen privaten Cloud (VPC) teilen oder ihnen die Möglichkeit geben, Objekte hochzuladen oder zu löschen.

Wenn Sie ein vorsigniertes Objekt mithilfe URL von AWS SDKs oder AWS Command Line Interface (AWS CLI) erstellen, verknüpfen Sie es URL mit einer bestimmten Aktion. Sie gewähren auch zeitlich begrenzten Zugriff auf die vorsignierte Datei, URL indem Sie eine benutzerdefinierte Ablaufzeit wählen, die so niedrig wie 1 Sekunde und maximal 7 Tage sein kann. Wenn Sie den Vorsignierten teilenURL, VPC kann die Person in der die Aktion so ausführen, URL als wäre sie der ursprüngliche signierende Benutzer. Wenn der seine Ablaufzeit URL erreicht hat, URL läuft der ab und funktioniert nicht mehr.

Wenn Sie eine vorsignierte Datei erstellenURL, müssen Sie Ihre Sicherheitsanmeldedaten und anschließend Folgendes angeben:

- Ein Access Point Amazon Resource Name (ARN) für den Amazon S3 on Outposts-Bucket
- Ein Objektschlüssel
- Eine HTTP Methode (PUTzum Hochladen von Objekten)
- Ein Verfallsdatum und eine Verfallszeit

Ein vorsignierter Wert URL ist nur für die angegebene Dauer gültig. Das heißt, Sie müssen die Aktion starten, die bis zum Datum und zur Uhrzeit URL vor dem Ablaufdatum zulässig ist. Sie können eine vorsignierte Option URL mehrfach verwenden, bis das Ablaufdatum und die Ablaufzeit erreicht sind. Wenn Sie ein vorsigniertes Token URL mithilfe eines temporären Tokens erstellt haben, URL läuft das ab, wenn das Token abläuft, auch wenn Sie das URL mit einer späteren Ablaufzeit erstellt haben.

Wenn die von einem vorsignierten Objekt erlaubte Aktion aus mehreren Schritten URL besteht, z. B. einem mehrteiligen Upload, müssen Sie alle Schritte vor Ablauf der Ablaufzeit starten. Wenn S3 auf Outposts versucht, einen Schritt mit einem abgelaufenen Wert zu startenURL, erhalten Sie eine Fehlermeldung.

Benutzer in der virtuellen privaten Cloud (VPC), die Zugriff auf die vorsignierten Dateien haben, URL können Objekte hochladen. Beispielsweise URL kann ein Benutzer in der Gruppe, der Zugriff auf VPC die vorsignierte Datei hat, ein Objekt in Ihren Bucket hochladen. Da Vorsignierte jedem

Benutzer, der Zugriff auf den vorsignierten Bucket hatVPC, Zugriff auf Ihren S3 on Outposts-Bucket URLs gewähren, empfehlen wir IhnenURL, diese entsprechend zu schützen. URLs Weitere Informationen zum Schutz URLs vorsignierter Personen finden Sie unter. [Einschränkung vordefinierter Funktionen URL](#)

Jeder, der über gültige Sicherheitsanmeldedaten verfügt, kann eine URL vorsignierte erstellen. Das Vorsignierte URL muss jedoch von einer Person erstellt werden, die berechtigt ist, den Vorgang auszuführen, auf dem das Vorsignierte URL basiert. Weitere Informationen finden Sie unter [Wer kann einen vorsignierten erstellen URL](#).

Verwenden von AWS SDKs, um eine URL für eine S3 in Outposts vorsignierte Objektoperation zu generieren

Java

SDKfür Java 2.x

Dieses Beispiel zeigt, wie Sie eine vorsignierte Datei generierenURL, mit der Sie ein Objekt für eine begrenzte Zeit in einen S3-Bucket auf Outposts hochladen können. Weitere Informationen finden Sie unter [Presigned URLs for S3 auf Outposts verwenden](#).

```
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 für Python (Boto3)

Dieses Beispiel zeigt, wie eine vorsignierte generiert wird URL, die für eine begrenzte Zeit eine S3-Aktion für Outposts ausführen kann. Weitere Informationen finden Sie unter [Presigned URLs for S3 auf Outposts verwenden](#). Verwenden Sie das Paket URL, um eine Anfrage mit dem zu stellen. 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 auf Outposts mit lokalem Amazon EMR on Outposts

Amazon EMR ist eine verwaltete Cluster-Plattform, die den Betrieb von Big-Data-Frameworks vereinfacht, wie Apache Hadoop and Apache Spark, AWS um riesige Datenmengen zu verarbeiten und zu analysieren. Mithilfe dieser Frameworks und verwandter Open-Source-Projekte können Sie Daten für Analysezwecke und Business Intelligence-Workloads verarbeiten. Amazon unterstützt Sie EMR auch bei der Transformation und Übertragung großer Datenmengen in und aus anderen AWS Datenspeichern und Datenbanken und unterstützt Amazon S3 on Outposts. Weitere Informationen zu Amazon EMR finden Sie unter [Amazon EMR on Outposts](#) im Amazon EMR Management Guide.

Für Amazon S3 auf Outposts EMR begann Amazon mit der Unterstützung von Apache Hadoop S3A-Anschluss in Version 7.0.0. Frühere Versionen von Amazon unterstützen EMR kein lokales S3 auf Outposts, und das EMR Dateisystem (EMRFS) wird nicht unterstützt.

Unterstützte Anwendungen

Amazon EMR with Amazon S3 on Outposts unterstützt die folgenden Anwendungen:

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

Weitere Informationen finden Sie im [Amazon EMR Release Guide](#).

Erstellen und konfigurieren Sie einen Amazon S3 on Outposts-Bucket

Amazon EMR verwendet AWS SDK for Java zusammen mit Amazon S3 on Outposts die, um Eingabedaten und Ausgabedaten zu speichern. Ihre EMR Amazon-Protokolldateien werden an einem von Ihnen ausgewählten regionalen Amazon S3-Standort gespeichert und nicht lokal auf Outpost gespeichert. Weitere Informationen finden Sie unter [EMRAmazon-Protokolle](#) im Amazon EMR Management Guide.

Um Amazon S3 und den DNS Anforderungen zu entsprechen, gelten für S3 on Outposts-Buckets Benennungsbeschränkungen und Einschränkungen. Weitere Informationen finden Sie unter [Erstellen eines S3-on-Outposts-Buckets](#).

Mit EMR Amazon-Version 7.0.0 und höher können Sie Amazon EMR mit S3 auf Outposts und dem S3A-Dateisystem verwenden.

Voraussetzungen

Berechtigungen für S3 on Outposts — Wenn Sie Ihr EMR Amazon-Instance-Profil erstellen, muss Ihre Rolle den Namespace AWS Identity and Access Management (IAM) für S3 auf Outposts enthalten. S3 auf Outposts hat seinen eigenen Namespace, `s3-outposts*`. Eine Beispielrichtlinie, die diesen Namespace verwendet, finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#)

S3A-Connector — Um Ihren EMR Cluster für den Zugriff auf Daten aus einem Amazon S3 on Outposts-Bucket zu konfigurieren, müssen Sie den Apache Hadoop S3A-Anschluss. Um den Connector zu verwenden, stellen Sie sicher, dass alle Ihre S3 das `s3a` Schema URIs verwenden. Wenn dies nicht der Fall ist, können Sie die Dateisystemimplementierung, die Sie für Ihren EMR Cluster verwenden, so konfigurieren, dass Ihr S3 mit dem S3A-Connector URIs funktioniert.

Um die Dateisystemimplementierung so zu konfigurieren, dass sie mit dem S3A-Connector funktioniert, verwenden Sie die `fs.file_scheme.impl` und `fs.AbstractFileSystem.file_scheme.impl` Konfigurationseigenschaften für Ihren EMR Cluster, wobei URIs dies dem S3-Typ `file_scheme` entspricht, den Sie haben. Um das folgende Beispiel zu verwenden, ersetzen Sie das *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen. Um beispielsweise die Dateisystemimplementierung für S3 zu ändern URIs, die das `s3` Schema verwenden, geben Sie die folgenden Cluster-Konfigurationseigenschaften an:

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

Um S3A zu verwenden, setzen Sie die `fs.file_scheme.impl` Konfigurationseigenschaft auf `org.apache.hadoop.fs.s3a.S3AFileSystem` und legen Sie

die `fs.AbstractFileSystem`.`file_scheme`.`impl` Eigenschaft auf `org.apache.hadoop.fs.s3a.S3A` fest.

Wenn Sie beispielsweise auf den Pfad zugreifers3a://*bucket*/... , setzen Sie die `fs.s3a.impl` Eigenschaft auf `org.apache.hadoop.fs.s3a.S3AFileSystem` und legen Sie die `fs.AbstractFileSystem.s3a.impl` Eigenschaft auf `org.apache.hadoop.fs.s3a.S3A` fest.

Erste Schritte bei der Nutzung von Amazon EMR mit Amazon S3 auf Outposts

In den folgenden Themen wird erklärt, wie Sie mit der Nutzung von Amazon EMR mit Amazon S3 auf Outposts beginnen können.

Themen

- [Erstellen einer Berechtigungsrichtlinie](#)
- [Ihren Cluster erstellen und konfigurieren](#)
- [Konfigurationsübersicht](#)
- [Überlegungen](#)

Erstellen einer Berechtigungsrichtlinie

Bevor Sie einen EMR Cluster erstellen können, der Amazon S3 auf Outposts verwendet, müssen Sie eine IAM Richtlinie erstellen, die an das EC2 Amazon-Instance-Profil für den Cluster angehängt wird. Die Richtlinie muss über Berechtigungen für den Zugriff auf den S3 on Outposts-Zugriffspunkt Amazon Resource Name (ARN) verfügen. Weitere Informationen zum Erstellen von IAM Richtlinien für S3 auf Outposts finden Sie unter [Einrichtung IAM mit S3 auf Outposts](#).

Die folgende Beispielrichtlinie zeigt, wie die erforderlichen Berechtigungen erteilt werden. Nachdem Sie die Richtlinie erstellt haben, fügen Sie die Richtlinie der Instanzprofilrolle hinzu, mit der Sie Ihren EMR Cluster erstellen, wie im [the section called "Ihren Cluster erstellen und konfigurieren"](#) Abschnitt beschrieben. Um dieses Beispiel zu verwenden, ersetzen Sie *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen.

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

Ihren Cluster erstellen und konfigurieren

Um einen Cluster zu erstellen, auf dem Spark mit S3 auf Outposts ausgeführt wird, führen Sie die folgenden Schritte in der Konsole aus.

Um einen Cluster zu erstellen, der läuft Spark mit S3 auf Outposts

1. Öffnen Sie die EMR Amazon-Konsole unter <https://console.aws.amazon.com/elasticmapreduce/>.
2. Wählen Sie im linken Navigationsbereich die Option Cluster aus.
3. Wählen Sie Cluster erstellen.
4. Für die EMR Amazon-Veröffentlichung wählen Sie emr-7.0.0 oder höher.
5. Wählen Sie für das Anwendungspaket die Option Spark interactive. Wählen Sie dann alle anderen unterstützten Anwendungen aus, die Sie in Ihren Cluster aufnehmen möchten.
6. Um Amazon S3 auf Outposts zu aktivieren, geben Sie Ihre Konfigurationseinstellungen ein.

Beispielkonfigurationseinstellungen

Um die folgenden Beispielkonfigurationseinstellungen zu verwenden, ersetzen Sie sie durch Ihre eigenen Informationen. *user input placeholders*

```
[  
  {  
    "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. Wählen Sie im Bereich Netzwerk eine virtuelle private Cloud (VPC) und ein Subnetz aus, die sich auf Ihrem AWS Outposts Rack befinden. Weitere Informationen zu Amazon EMR on Outposts finden Sie unter [EMRClusters on AWS Outposts](#) im Amazon EMR Management Guide.
8. Wählen Sie im EMR Abschnitt EC2Instanzprofil für Amazon die IAM Rolle aus, der die [zuvor erstellte Berechtigungsrichtlinie](#) angehängt ist.
9. Konfigurieren Sie Ihre verbleibenden Cluster-Einstellungen und wählen Sie dann Create cluster aus.

Konfigurationsübersicht

In der folgenden Tabelle werden S3A-Konfigurationen und die Werte beschrieben, die für ihre Parameter angegeben werden müssen, wenn Sie einen Cluster einrichten, der S3 auf Outposts mit Amazon verwendet. EMR

Parameter	Standardwert	Erforderlicher Wert für S3 auf Outposts	Erklärung
<code>fs.s3a.aws.credentials.provider</code>	Wenn nicht angegeben, sucht S3A im Region-Bucket nach S3 mit dem Outposts-Bucket-Namen.	Der Access Point ARN des S3 on Outposts Buckets	Amazon S3 on Outposts unterstützt ausschließlich virtuelle private Cloud-Zugriffspunkte (VPC) als einzige Möglichkeit, auf Ihre Outposts-Buckets zuzugreifen.
<code>fs.s3a.committer.name</code>	<code>file</code>	<code>magic</code>	Magic Committer ist der einzige unterstützte Committer für S3 auf Outposts.
<code>fs.s3a.select.enabled</code>	<code>TRUE</code>	<code>FALSE</code>	S3 Select wird auf Outposts nicht unterstützt.
<code>JAVA_HOME</code>	<code>/usr/lib/jvm/java-8</code>	<code>/usr/lib/jvm/java-11-amazon-corretto.x86_64</code>	S3 auf Outposts auf S3A erfordert Java Version 11.

In der folgenden Tabelle wird beschrieben Spark Konfigurationen und die Werte, die für ihre Parameter angegeben werden müssen, wenn Sie einen Cluster einrichten, der S3 auf Outposts mit Amazon EMR verwendet.

Parameter	Standardwert	Erforderlicher Wert für S3 auf Outposts	Erklärung
<code>spark.sql.sources.fastS3PartitionDiscovery.enabled</code>	TRUE	FALSE	S3 auf Outposts unterstützt keine schnelle Partition.
<code>spark.executorEnv.JAVA_HOME</code>	<code>/usr/lib/jvm/java-8</code>	<code>/usr/lib/jvm/java-11-amazon-corretto.x86_64</code>	S3 auf Outposts auf S3A erfordert Java-Version 11.

Überlegungen

Beachten Sie Folgendes, wenn Sie Amazon EMR mit S3 in Outposts-Buckets integrieren:

- Amazon S3 on Outposts wird mit EMR Amazon-Version 7.0.0 und höher unterstützt.
- Der S3A-Connector ist erforderlich, um S3 auf Outposts mit Amazon zu verwenden. EMR Nur S3A verfügt über die Funktionen, die für die Interaktion mit S3 in Outposts-Buckets erforderlich sind. [Informationen zur Einrichtung des S3A-Connectors finden Sie unter Voraussetzungen.](#)
- Amazon S3 on Outposts unterstützt nur serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) bei Amazon. EMR Weitere Informationen finden Sie unter [the section called "Datenverschlüsselung"](#).
- Amazon S3 on Outposts unterstützt keine Schreibvorgänge mit dem FileOutputStream S3A. Schreibvorgänge mit dem S3A FileOutputStream auf S3 auf Outposts-Buckets führen zu dem folgenden Fehler InvalidStorageClass: Die von Ihnen angegebene Speicherklasse ist nicht gültig.
- Amazon S3 on Outposts wird mit Amazon EMR Serverless oder Amazon EMR on nicht unterstützt. EKS
- EMRAmazon-Protokolle werden an einem von Ihnen ausgewählten regionalen Amazon S3-Standort gespeichert und nicht lokal im S3 on Outposts-Bucket gespeichert.

Autorisierungs- und Authentifizierungs-Caching

S3 on Outposts speichert Authentifizierungs- und Autorisierungsdaten sicher lokal in Outposts-Racks. Der Cache entfernt für jede Anfrage Roundtrips AWS-Region zum übergeordneten Objekt. Dadurch entfällt die Variabilität, die durch Netzwerk-Roundtrips entsteht. Mit dem Authentifizierungs- und Autorisierungs-Cache in S3 auf Outposts erhalten Sie konsistente Latenzen, die unabhängig von der Latenz der Verbindung zwischen den Outposts und den. AWS-Region

Wenn Sie eine S3 on API Outposts-Anfrage stellen, werden die Authentifizierungs- und Autorisierungsdaten sicher zwischengespeichert. Die zwischengespeicherten Daten werden dann verwendet, um nachfolgende S3-Objektanforderungen zu authentifizieren. API S3 on Outposts speichert Authentifizierungs- und Autorisierungsdaten nur dann zwischen, wenn die Anfrage mit Signature Version 4A (Sigv4A) signiert wurde. Der Cache wird lokal auf den Outposts innerhalb des S3 on Outposts-Dienstes gespeichert. Er wird asynchron aktualisiert, wenn Sie eine S3-Anfrage stellen. API Der Cache ist verschlüsselt und es werden keine kryptografischen Klartext-Schlüssel auf Outposts gespeichert.

Der Cache ist bis zu 10 Minuten gültig, wenn der Outpost mit dem verbunden ist. AWS-Region Es wird asynchron aktualisiert, wenn Sie eine S3 on API Outposts-Anfrage stellen, um sicherzustellen, dass die neuesten Richtlinien verwendet werden. Wenn der Outpost vom getrennt wird AWS-Region, ist der Cache bis zu 12 Stunden gültig.

Konfiguration des Autorisierungs- und Authentifizierungscaches

S3 on Outposts speichert automatisch Authentifizierungs- und Autorisierungsdaten für Anfragen, die mit dem SigV4A-Algorithmus signiert wurden. Weitere Informationen finden Sie im Benutzerhandbuch unter [Signieren von AWS API Anfragen](#).AWS Identity and Access Management Der SigV4A-Algorithmus ist in den neuesten Versionen von verfügbar. AWS SDKs Sie können ihn über eine Abhängigkeit von den [AWS Common Runtime \(CRT\)](#) -Bibliotheken abrufen.

Sie müssen die neueste Version von verwenden AWS SDK und die neueste Version von installierenCRT. Sie können beispielsweise ausführen, `pip install awscrt` um die neueste Version von CRT mit Boto3 zu erhalten.

S3 on Outposts speichert keine Authentifizierungs- und Autorisierungsdaten für Anfragen, die mit dem SigV4-Algorithmus signiert wurden.

Die SigV4a-Signatur wird validiert

Sie können AWS CloudTrail damit überprüfen, ob Anfragen mit SigV4a signiert wurden. Weitere Informationen CloudTrail zur Einrichtung von S3 auf Outposts finden Sie unter [Überwachen von S3 in Outposts mit Protokollen in AWS CloudTrail](#).

Nachdem Sie die Konfiguration vorgenommen haben CloudTrail, können Sie im `SignatureVersion` Feld der CloudTrail Protokolle überprüfen, wie eine Anfrage signiert wurde. Für Anfragen, die mit SigV4a signiert wurden, ist der Wert `SignatureVersion` auf `AWS_4_ECDSA_P256_SHA256` gesetzt. Für Anfragen, die mit SigV4 signiert wurden, wird der Wert auf `AWS_4_HMAC_SHA256` gesetzt.

Sicherheit in S3 on Outposts

Cloud-Sicherheit hat AWS höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der [AWS](#) . Weitere Informationen zu den Compliance-Programmen, die für Amazon S3 auf Outposts gelten, finden Sie unter [AWS Services in Scope by Compliance Program AWS](#) .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von S3 on Outposts zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Sie S3 on Outposts zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie lernen auch, wie Sie andere verwenden können AWS-Services , die Ihnen helfen, Ihre S3 on Outposts-Ressourcen zu überwachen und zu sichern.

Themen

- [Einrichtung IAM mit S3 auf Outposts](#)
- [Datenverschlüsselung in S3 on Outposts](#)
- [AWS PrivateLink für S3 auf Outposts](#)
- [AWS Authentifizierungsspezifische Richtlinienschlüssel für Signature Version 4 \(Sigv4\)](#)
- [AWS verwaltete Richtlinien für Amazon S3 auf Outposts](#)
- [Verwenden von serviceverknüpften Rollen für S3 on Outposts](#)

Einrichtung IAM mit S3 auf Outposts

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon S3 on Outposts-Ressourcen zu verwenden. IAM ist eine AWS-Service, die Sie ohne zusätzliche Kosten nutzen können. Standardmäßig haben IAM-Benutzer keine Berechtigungen für S3 auf Outpost-Ressourcen und -Vorgänge. Um Zugriffsberechtigungen für S3 auf Outposts-Ressourcen und API -Operationen IAM zu gewähren, können Sie [Benutzer](#), [Gruppen](#) oder [Rollen](#) erstellen und Berechtigungen anhängen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter [Erstellen eines Berechtigungssatzes](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, IAM die über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Folgen Sie den Anweisungen [unter Erstellen einer Rolle für einen externen Identitätsanbieter \(Federation\)](#) im IAMBenutzerhandbuch.

- IAMBenutzer:

- Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen [unter Eine Rolle für einen IAM Benutzer erstellen](#) im IAMBenutzerhandbuch.
- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Folgen Sie den Anweisungen [unter Hinzufügen von Berechtigungen für einen Benutzer \(Konsole\)](#) im IAMBenutzerhandbuch.

Zusätzlich zu IAM identitätsbasierten Richtlinien unterstützt S3 on Outposts sowohl Bucket- als auch Access-Point-Richtlinien. Bucket-Richtlinien und Zugriffspunkt-Richtlinien sind [ressourcenbasierte Richtlinien](#), die mit der S3-on-Outposts-Ressource verbunden sind.

- Eine Bucket-Richtlinie ist mit dem Bucket verknüpft und erlaubt oder verweigert Anfragen an den Bucket und die darin enthaltenen Objekte auf der Grundlage der Elemente in der Richtlinie.
- Im Gegensatz dazu ist eine Zugriffspunkt-Richtlinie mit dem Zugriffspunkt verbunden und erlaubt oder verweigert Anfragen an den Zugriffspunkt.

Die Zugriffspunkt-Richtlinie funktioniert mit der Bucket-Richtlinie, die dem zugrunde liegenden S3-on-Outposts-Bucket zugeordnet ist. Damit eine Anwendung oder ein Benutzer über einen S3-on-Outposts-Zugriffspunkt auf Objekte in einem S3-on-Outposts-Bucket zugreifen kann, müssen sowohl die Zugriffspunkt- als auch die Bucket-Richtlinie die Anfrage zulassen.

Einschränkungen, die Sie in eine Zugriffspunktrichtlinie einschließen, gelten nur für Anforderungen, die über diesen Zugriffspunkt eingehen. Wenn beispielsweise ein Zugriffspunkt mit einem Bucket verbunden ist, können Sie die Zugriffspunkt-Richtlinie nicht verwenden, um Anfragen, die direkt an den Bucket gerichtet sind, zuzulassen oder zu verweigern. Einschränkungen, die Sie auf eine Bucket-Richtlinie anwenden, können jedoch Anfragen zulassen oder verweigern, die direkt an den Bucket oder über den Zugriffspunkt gestellt werden.

In einer IAM Richtlinie oder einer ressourcenbasierten Richtlinie definieren Sie, welche S3-Aktionen auf Outposts zulässig oder verweigert werden. S3-Aktionen für Outposts entsprechen spezifischen S3-Vorgängen für OutpostsAPI. Aktionen von S3 on Outposts verwenden das Namespace-Präfix `s3-outposts:`. Anfragen an das S3 on Outposts-Steuerelement API in einem AWS-Region und Anfragen an die API Objektendpunkte auf dem Outpost werden mithilfe des Namespace-Präfixes authentifiziert IAM und anhand dieses autorisiert. `s3-outposts:` Um mit S3 auf Outposts zu arbeiten, konfigurieren Sie Ihre IAM Benutzer und autorisieren Sie sie für den `s3-outposts:` IAM Namespace.

Weitere Informationen finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 on Outposts](#) in der Service-Autorisierungs-Referenz.

Note

- Zugriffskontrolllisten (ACLs) werden von S3 on Outposts nicht unterstützt.
- S3 on Outposts setzt standardmäßig den Bucket-Besitzer als Objekteigentümer ein, um sicherzustellen, dass der Eigentümer eines Buckets nicht am Zugriff auf oder am Löschen von Objekten gehindert werden kann.
- In S3 on Outposts ist S3 Block Public Access stets aktiviert, um sicherzustellen, dass nie öffentlich auf Objekte zugegriffen werden kann.

Weitere Informationen IAM zur Einrichtung von S3 auf Outposts finden Sie in den folgenden Themen.

Themen

- [Prinzipale für die Richtlinien von S3 on Outposts](#)

- [Ressource ARNs für S3 auf Outposts](#)
- [Beispielrichtlinien für S3 on Outposts](#)
- [Berechtigungen für S3-on-Outposts-Endpunkte](#)
- [Serviceverknüpfte Rollen für S3 on Outposts](#)

Prinzipale für die Richtlinien von S3 on Outposts

Wenn Sie eine ressourcenbasierte Richtlinie erstellen, um Zugriff auf Ihren S3-on-Outposts-Bucket zu gewähren, müssen Sie das `Principal`-Element verwenden, um die Person oder Anwendung anzugeben, die eine Anfrage für eine Aktion oder einen Vorgang auf dieser Ressource stellen kann. Für S3-on-Outposts-Richtlinien können Sie einen der folgenden Prinzipals verwenden:

- Ein AWS-Konto
- Ein IAM Nutzer
- Eine IAM Rolle
- Alle Prinzipale durch Angabe eines Platzhalters (*) in einer Richtlinie, die ein `Condition`-Element zur Beschränkung des Zugriffs auf einen bestimmten IP-Bereich verwendet

Important

Sie können keine Richtlinie für einen S3-on-Outposts-Bucket schreiben, die einen Platzhalter (*) im `Principal`-Element verwendet, es sei denn, die Richtlinie enthält auch eine `Condition`, die den Zugriff auf einen bestimmten IP-Bereich beschränkt. Mit dieser Beschränkung wird sichergestellt, dass es keinen öffentlichen Zugriff auf Ihren S3-on-Outposts-Bucket gibt. Ein Beispiel finden Sie unter [Beispielrichtlinien für S3 on Outposts](#).

Weitere Informationen zu diesem `Principal` Element finden Sie unter [AWS JSONPolicy Elements: Principal](#) im IAMBenutzerhandbuch.

Ressource ARNs für S3 auf Outposts

Amazon-Ressourcennamen (ARNs) für S3 auf Outposts enthalten die Outpost-ID zusätzlich zu der AWS-Region, auf die sich der Outpost bezieht, der AWS-Konto ID und dem Ressourcennamen. Um auf Ihre Outposts-Buckets und Objekte zuzugreifen und Aktionen für diese auszuführen, müssen Sie eines der in der folgenden Tabelle aufgeführten ARN Formate verwenden.

Der *partition* Wert in der ARN bezieht sich auf eine Gruppe von AWS-Regionen. Jeder AWS-Konto ist auf eine Partition beschränkt. Im Folgenden werden die unterstützten Partitionen angezeigt:

- aws – AWS-Regionen
- aws-us-gov— Regionen AWS GovCloud (US)

Die folgende Tabelle zeigt S3 in den ARN Outposts-Formaten.

Amazon S3 auf Outposts ARN	ARNformatieren	Beispiel
Eimer ARN	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i> / bucket/ <i>bucket_name</i>	arn:aws:s3-outposts: <i>us-west-2</i> :123456789012 :outpost/ <i>op-01ac5d28a6a232904</i> / bucket/ <i>amzn-s3-demo-bucket1</i>
Zugangspunkt ARN	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i> /accesspoint/ <i>accesspoint_name</i>	arn:aws:s3-outposts: <i>us-west-2</i> :123456789012 :outpost/ <i>op-01ac5d28a6a232904</i> /accesspoint/ <i>access-point-name</i>
Objekt ARN	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>	arn:aws:s3-outposts: <i>us-west-2</i> :123456789012 :outpost/ <i>op-01ac5d28a6a232904</i> / bucket/ <i>amzn-s3-demo-bucket1</i> /object/ <i>myobject</i>

Amazon S3 auf Outposts ARN	ARNformatieren	Beispiel
Zugriffspunktobjekt S3 on Outposts ARN (wird in Richtlinien verwendet)	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>	arn:aws:s3-outposts: <i>us-west-2</i> : <i>123456789012</i> :outpost/ <i>op-01ac5d28a6a232904</i> /accesspoint/ <i>access-point-name/object/myobject</i>
S3 auf Outposts ARN	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i>	arn:aws:s3-outposts: <i>us-west-2</i> : <i>123456789012</i> :outpost/ <i>op-01ac5d28a6a232904</i>

Beispielrichtlinien für S3 on Outposts

Example : Bucket-Richtlinie für S3 auf Outposts mit einem Principal AWS-Konto

Die folgende Bucket-Richtlinie verwendet einen AWS-Konto Principal, um Zugriff auf einen S3 on Outposts-Bucket zu gewähren. Wenn Sie diese Bucket-Richtlinie verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre eigenen Informationen.

```
{
  "Version": "2012-10-17",
  "Id": "ExampleBucketPolicy1",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "123456789012"
      },
      "Action": "s3-outposts:*",
      "Resource": "arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket"
    }
  ]
}
```

```
]
}
```

Example : S3-on-Outposts-Bucket-Richtlinie mit Platzhalterprinzipal (*) und Bedingungsschlüssel, um den Zugriff auf einen bestimmten IP-Bereich zu beschränken

Die folgende Bucket-Richtlinie verwendet einen Platzhalterprinzipal (*) mit der `aws:SourceIp`-Bedingung, um den Zugriff auf einen bestimmten IP-Bereich zu beschränken. Wenn Sie diese Bucket-Richtlinie verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre eigenen Informationen.

```
{
  "Version": "2012-10-17",
  "Id": "ExampleBucketPolicy2",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": { "AWS" : "*" },
      "Action": "s3-outposts:*",
      "Resource": "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket",
      "Condition" : {
        "IpAddress" : {
          "aws:SourceIp": "192.0.2.0/24"
        },
        "NotIpAddress" : {
          "aws:SourceIp": "198.51.100.0/24"
        }
      }
    }
  ]
}
```

Berechtigungen für S3-on-Outposts-Endpunkte

S3 on Outposts benötigt eigene Berechtigungen für die Verwaltung von S3 on Outposts-Endpunktaktionen. IAM


Note

- Für Endpunkte, die den Zugriffstyp des kundeneigenen IP-Adresspools (CoIP-Pool) verwenden, müssen Sie außerdem über Berechtigungen zum Arbeiten mit IP-Adressen aus Ihrem CoIP-Pool verfügen, wie in der folgenden Tabelle beschrieben.
- Für gemeinsame Konten, die über Outposts auf S3 zugreifen AWS Resource Access Manager, können Benutzer mit diesen gemeinsamen Konten keine eigenen Endpunkte in einem gemeinsamen Subnetz erstellen. Wenn ein Benutzer in einem freigegebenen Konto seine eigenen Endpunkte verwalten möchte, muss das freigegebene Konto ein eigenes Subnetz in Outposts erstellen. Weitere Informationen finden Sie unter [the section called “Freigabe von S3 on Outposts”](#).

Die folgende Tabelle zeigt die IAM endpunktbezogenen Berechtigungen von S3 on Outposts.

Aktion	IAMBerechtigungen
CreateEndpoint	s3-outposts:CreateEndpoint ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeVpcs ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:CreateTags iam:CreateServiceLinkedRole Für Endpunkte, die den Zugriffstyp des kundeneigenen On-Premises-IP-Adresspools (CoIP-Pool) verwenden, sind die folgenden zusätzlichen Berechtigungen erforderlich: s3-outposts:CreateEndpoint

Aktion	IAMBerechtigungen
	ec2:DescribeCoipPools ec2:GetCoipPoolUsage ec2:AllocateAddress ec2:AssociateAddress ec2:DescribeAddresses ec2:DescribeLocalGatewayRouteTableVpcAssociations
DeleteEndpoint	s3-outposts:DeleteEndpoint ec2>DeleteNetworkInterface ec2:DescribeNetworkInterfaces Für Endpunkte, die den Zugriffstyp des kundeneigenen On-Premises-IP-Adresspools (CoIP-Pool) verwenden, sind die folgenden zusätzlichen Berechtigungen erforderlich: s3-outposts:DeleteEndpoint ec2:DisassociateAddress ec2:DescribeAddresses ec2:ReleaseAddress
ListEndpoints	s3-outposts:ListEndpoints

 Note

Sie können Ressourcen-Tags in einer IAM Richtlinie verwenden, um Berechtigungen zu verwalten.

Serviceverknüpfte Rollen für S3 on Outposts

S3 on Outposts verwendet IAM dienstbezogene Rollen, um einige Netzwerkressourcen in Ihrem Namen zu erstellen. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für S3 on Outposts](#).

Datenverschlüsselung in S3 on Outposts

Standardmäßig werden alle in Amazon S3 auf Outposts gespeicherten Daten mithilfe einer serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt. Weitere Informationen finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln \(SSE-S3\)](#) im Amazon S3 S3-Benutzerhandbuch.

Sie können optional serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (-C) verwenden. Um SSE -C zu verwenden, geben Sie einen Verschlüsselungsschlüssel als Teil Ihrer Objektanforderungen an. Die serverseitige Verschlüsselung verschlüsselt nur die Objektdaten, nicht die Metadaten des Objekts. Weitere Informationen finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln](#) im Amazon S3 S3-Benutzerhandbuch.

Note

S3 on Outposts unterstützt keine serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) -Schlüsseln (SSE-KMS).

AWS PrivateLink für S3 auf Outposts

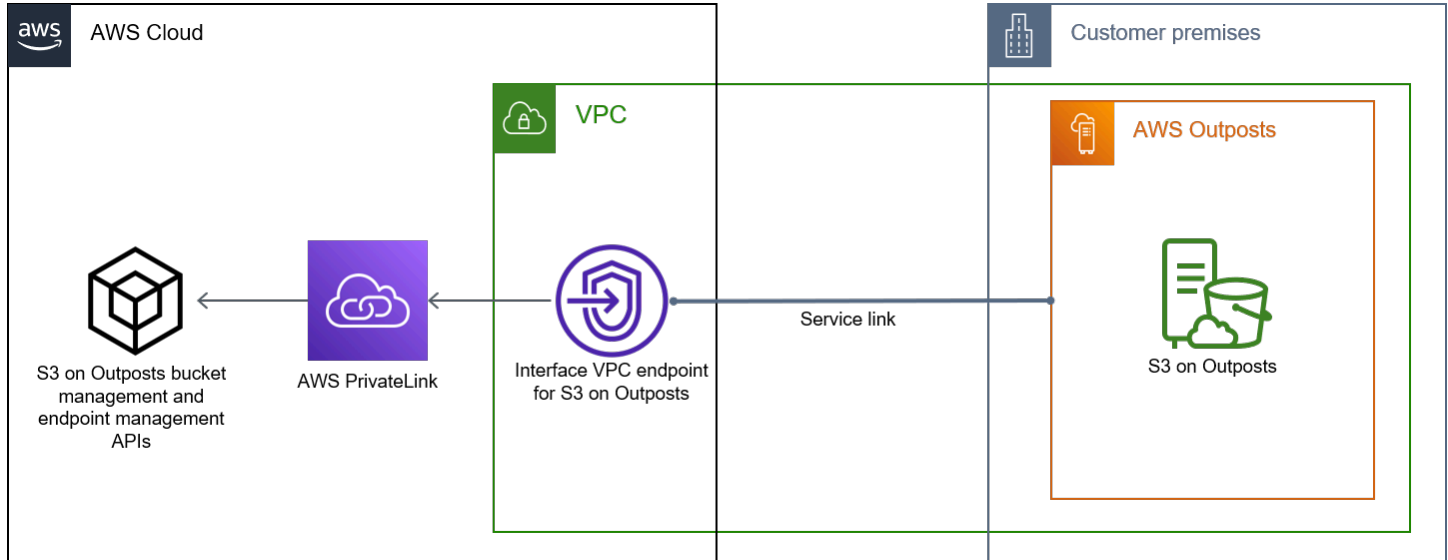
S3 on Outposts unterstützt AWS PrivateLink, was direkten Verwaltungszugriff auf Ihren S3 on Outposts-Speicher über einen privaten Endpunkt in Ihrem virtuellen privaten Netzwerk ermöglicht. Auf diese Weise können Sie Ihre interne Netzwerkarchitektur vereinfachen und Verwaltungsvorgänge auf Ihrem Outposts-Objektspeicher durchführen, indem Sie private IP-Adressen in Ihrer Virtual Private Cloud (VPC) verwenden. Durch die Verwendung AWS PrivateLink entfällt die Notwendigkeit, öffentliche IP-Adressen oder Proxyserver zu verwenden.

[Mit AWS PrivateLink for Amazon S3 on Outposts können Sie VPC-Schnittstellenendpunkte in Ihrer virtuellen privaten Cloud \(VPC\) bereitstellen, um auf Ihr S3 auf Outposts Bucket Management](#)

[und Endpoint Management zuzugreifen](#). APIs auf VPC Schnittstellen-Endpunkte kann direkt von Anwendungen aus zugegriffen werden, die bei Ihnen VPC oder vor Ort über Ihr virtuelles privates Netzwerk () oder bereitgestellt werden. VPN AWS Direct Connect Sie können über auf das Bucket- und Endpunktmanagement APIs zugreifen AWS PrivateLink. AWS PrivateLink unterstützt keine [API-Datenübertragungsvorgänge](#) wie GETPUT, und ähnliches APIs. Diese Vorgänge werden bereits privat über die Konfiguration des S3-on-Outposts-Endpunkts und des Zugriffspunkts übertragen. Weitere Informationen finden Sie unter [Vernetzung für S3 on Outposts](#).

Schnittstellenendpunkte werden durch eine oder mehrere elastische Netzwerkschnittstellen (ENIs) repräsentiert, denen private IP-Adressen aus Subnetzen in Ihrem zugewiesen werden. VPC Anfragen an Schnittstellenendpunkte für S3 on Outposts werden automatisch an S3 on Outposts Bucket und Endpoint Management APIs im Netzwerk weitergeleitet. AWS Sie können auch über oder () auf Schnittstellenendpunkte in Ihren lokalen Anwendungen VPC zugreifen. AWS Direct Connect AWS Virtual Private Network AWS VPN [Weitere Informationen dazu, wie Sie Ihr Netzwerk VPC mit Ihrem lokalen Netzwerk verbinden, finden Sie im AWS Direct Connect Benutzerhandbuch und im AWS Site-to-Site VPN Benutzerhandbuch](#).

Schnittstellenendpunkte leiten Anfragen für S3 im Outposts-Bucket und Endpoint Management APIs über das AWS Netzwerk und durch das Netzwerk weiter AWS PrivateLink, wie in der folgenden Abbildung dargestellt.



Allgemeine Informationen zu Schnittstellenendpunkten finden Sie im Handbuch unter [VPC Schnittstellenendpunkte \(AWS PrivateLink\)](#). AWS PrivateLink

Themen

- [Beschränkungen und Einschränkungen](#)

- [Zugriff auf S3-on-Outposts-Schnittstellenendpunkte](#)
- [Aktualisierung einer lokalen Konfiguration DNS](#)
- [Einen VPC Endpunkt für S3 auf Outposts erstellen](#)
- [Bucket-Richtlinien und VPC Endpunktrichtlinien für S3 auf Outposts erstellen](#)

Beschränkungen und Einschränkungen

Wenn Sie über Outposts Bucket und Endpoint Management auf S3 APIs zugreifen AWS PrivateLink, gelten VPC Einschränkungen. Weitere Informationen finden Sie unter [Interface endpoint properties and limitations \(Eigenschaften und Beschränkungen von Schnittstellen-Endpunkten\)](#) und [AWS PrivateLink quotas \(PrivateLink-Kontingente\)](#) im AWS PrivateLink -Leitfaden.

Darüber hinaus unterstützt es Folgendes AWS PrivateLink nicht:

- [Endpunkte nach dem Federal Information Processing Standard \(FIPS\)](#)
- [S3 auf Outposts APIs, Datenübertragung](#), zum Beispiel, GETPUT, und ähnliche API Objektoperationen.
- Privat DNS

Zugriff auf S3-on-Outposts-Schnittstellenendpunkte

Um APIs mithilfe von Outposts Bucket und Endpoint Management auf S3 zuzugreifen AWS PrivateLink, müssen Sie Ihre Anwendungen so aktualisieren, dass sie endpunktspezifische Namen DNS verwenden. Wenn Sie einen Schnittstellenendpunkt erstellen, werden zwei Typen von endpunktspezifischen S3-Namen für Outposts AWS PrivateLink generiert: Regional und Zonal.

- Regionale DNS Namen — beinhalten eine eindeutige VPC Endpunkt-ID, eine Service-ID, die und AWS-Region `vpce.amazonaws.com`, zum Beispiel. `vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com`
- Zonale DNS Namen — beinhalten eine eindeutige VPC Endpunkt-ID, die Availability Zone, eine Service-ID, die AWS-Region, und `vpce.amazonaws.com`, zum Beispiel. `vpce-1a2b3c4d-5e6f-us-east-1a.s3-outposts.us-east-1.vpce.amazonaws.com` Sie können diese Option verwenden, wenn Ihre Architektur Availability Zones isoliert. Beispielsweise könnten Sie zonale DNS Namen zur Fehlereindämmung oder zur Senkung der regionalen Datenübertragungskosten verwenden.

⚠ Important

Die Endpunkte der Schnittstelle S3 auf Outposts werden DNS gemeinfrei aufgelöst. S3 on Outposts unterstützt Private DNS nicht. Verwenden Sie den `--endpoint-url` Parameter für das gesamte Bucket- und EndpunktmanagementAPIs.

AWS CLI Beispiele

Verwenden Sie die `--endpoint-url` Parameter `--region` und, um APIs über S3 auf Endpunkten der Outposts-Schnittstelle auf Bucket Management und Endpoint Management zuzugreifen.

Example : Verwenden Sie den EndpunktURL, um Buckets mit dem S3-Steurelement aufzulisten API

Ersetzen Sie im folgenden Beispiel die Region `us-east-1`, den VPC Endpunkt URL `vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com` und die Konto-ID `111122223333` durch die entsprechenden Informationen.

```
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
```

AWS SDK Beispiele

Aktualisieren Sie Ihre Version SDKs auf die neueste Version und konfigurieren Sie Ihre Clients so, dass sie einen Endpunkt URL für den Zugriff auf die S3-Steuerung API für S3 auf den Endpunkten Outposts Outposts-Schnittstelle verwenden.

SDK for Python (Boto3)

Example : Verwenden Sie einen EndpunktURL, um auf die S3-Steuerung zuzugreifen API

Ersetzen Sie im folgenden Beispiel die Region `us-east-1` und den VPC Endpunkt URL `vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com` durch die entsprechenden Informationen.

```
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'  
)
```

Weitere Informationen finden Sie unter [AWS PrivateLink für Amazon S3](#) im Boto3-Entwicklerhandbuch.

SDK for Java 2.x

Example : Verwenden Sie einen EndpunktURL, um auf das S3-Steuererelement zuzugreifen API

Ersetzen Sie im folgenden Beispiel den VPC Endpunkt URL *vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com* und die Region *Region.US_EAST_1* durch die entsprechenden Informationen.

```
// 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()
```

Weitere Informationen finden Sie [S3ControlClient](#) in der AWS SDK for Java APIReferenz.

Aktualisierung einer lokalen Konfiguration DNS

Wenn Sie endpunktspezifische DNS Namen für den Zugriff auf die Schnittstellenendpunkte für S3 auf Outposts Bucket Management und Endpoint Management verwenden APIs, müssen Sie Ihren lokalen Resolver nicht aktualisieren. DNS Sie können den endpunktspezifischen DNS Namen mit der privaten IP-Adresse des Schnittstellenendpunkts aus der öffentlichen Domäne S3 on DNS Outposts auflösen.

Einen VPC Endpunkt für S3 auf Outposts erstellen

Informationen zum Erstellen eines VPC Schnittstellenendpunkts für S3 auf Outposts finden Sie unter [Erstellen eines VPC Endpunkts](#) im AWS PrivateLink Handbuch.

Bucket-Richtlinien und VPC Endpunktrichtlinien für S3 auf Outposts erstellen

Sie können Ihrem VPC Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf S3 auf Outposts steuert. Sie können die `aws:sourceVpce` Bedingung in den Bucket-Richtlinien von S3 on Outposts auch verwenden, um den Zugriff auf bestimmte Buckets von einem bestimmten VPC Endpunkt aus zu beschränken. Mit VPC Endpunktrichtlinien können Sie den Zugriff auf S3 über Outposts Bucket Management APIs und Endpoint Management APIs kontrollieren. Mit Bucket-Richtlinien können Sie den Zugriff auf das S3 im Bucket-Management APIs von Outposts kontrollieren. Sie können jedoch den Zugriff auf Objektaktionen für S3 on Outposts nicht mit `aws:sourceVpce` verwalten.

Zugriffsrichtlinien für S3 on Outposts enthalten die folgenden Informationen:

- Der Prinzipal AWS Identity and Access Management (IAM), für den Aktionen erlaubt oder verweigert werden.
- Die S3-Steuerungsaktionen, die erlaubt oder verweigert werden.
- Die S3-on-Outposts-Ressourcen, für die Aktionen erlaubt oder verweigert werden.

Die folgenden Beispiele zeigen Richtlinien, die den Zugriff auf einen Bucket oder einen Endpunkt einschränken. Weitere Informationen zur VPC Konnektivität finden Sie unter [Network-to-VPC Konnektivitätsoptionen](#) im AWS Whitepaper [Amazon Virtual Private Cloud Connectivity Options](#).

Important

- Wenn Sie die in diesem Abschnitt beschriebenen Beispielrichtlinien für VPC Endgeräte anwenden, können Sie Ihren Zugriff auf den Bucket blockieren, ohne dies zu beabsichtigen. Bucket-Berechtigungen, die den Bucket-Zugriff auf Verbindungen beschränken, die von Ihrem VPC Endpunkt ausgehen, können alle Verbindungen zum Bucket blockieren. Informationen zur Behebung dieses Problems finden Sie unter [Meine Bucket-Richtlinie hat die falsche VPC oder die VPC Endpunkt-ID. Wie kann ich die Richtlinie so ändern, dass ich auf den Bucket zugreifen kann?](#) im AWS Support Knowledge Center.
- Bevor Sie die folgenden Beispiel-Bucket-Richtlinien verwenden, ersetzen Sie die VPC Endpunkt-ID durch einen Wert, der Ihrem Anwendungsfall entspricht. Andernfalls können Sie nicht auf Ihren Bucket zugreifen.

- Wenn Ihre Richtlinie den Zugriff auf einen S3 on Outposts-Bucket nur von einem bestimmten VPC Endpunkt aus erlaubt, deaktiviert sie den Konsolenzugriff für diesen Bucket, da Konsolenanfragen nicht vom angegebenen VPC Endpunkt stammen.

Themen

- [Beispiel: Beschränken des Zugriffs auf einen bestimmten Bucket von einem Endpunkt aus VPC](#)
- [Beispiel: Verweigern des Zugriffs von einem bestimmten VPC Endpunkt aus in einer S3-Bucket-Richtlinie auf Outposts](#)

Beispiel: Beschränken des Zugriffs auf einen bestimmten Bucket von einem Endpunkt aus VPC

Sie können eine Endpunktrichtlinie erstellen, die den Zugriff auf bestimmte S3-on-Outposts-Buckets beschränkt. Die folgende Richtlinie beschränkt den Zugriff für die `GetBucketPolicy` Aktion nur auf die *example-outpost-bucket*. Zum Verwenden dieses Beispiels ersetzen Sie die Beispielwerte durch Ihre eigenen.

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

Beispiel: Verweigern des Zugriffs von einem bestimmten VPC Endpunkt aus in einer S3-Bucket-Richtlinie auf Outposts

Die folgende Bucket-Richtlinie für S3 on Outposts verweigert den Zugriff `GetBucketPolicy` auf den *example-outpost-bucket* Bucket über den *vpce-1a2b3c4d* VPC Endpunkt.

Die `aws:sourceVpce` Bedingung spezifiziert den Endpunkt und erfordert keinen Amazon-Ressourcennamen (ARN) für die VPC Endpunktressource, sondern nur die Endpunkt-ID. Zum Verwenden dieses Beispiels ersetzen Sie die Beispielwerte durch Ihre eigenen.

```
{
  "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:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outpost-
bucket",
      "Condition": {
        "StringEquals": {"aws:sourceVpce": "vpce-1a2b3c4d"}
      }
    }
  ]
}
```

AWS Authentifizierungsspezifische Richtlinienchlüssel für Signature Version 4 (Sigv4)

Die folgende Tabelle zeigt die Bedingungsschlüssel für die Authentifizierung mit AWS Signature Version 4 (Sigv4), die Sie mit Amazon S3 on Outposts verwenden können. In einer Bucket-Richtlinie können Sie diese Bedingungen hinzufügen, um ein bestimmtes Verhalten zu erzwingen, wenn Anforderungen mit der Signature Version 4 authentifiziert werden. Beispiele für Richtlinien finden Sie unter [Beispiele für Bucket-Richtlinien, die mit der Signature Version 4 verbundene Bedingungsschlüssel verwenden](#). Weitere Informationen zur Authentifizierung von Anfragen mit Signature Version 4 finden Sie unter [Authentifizieren von Anfragen \(AWS Signature Version 4\)](#) in der Amazon Simple Storage Service Reference API

Anwendbare Schlüssel	Beschreibung
s3-outposts:authType	<p>S3 on Outposts unterstützt verschiedene Methoden der Authentifizierung. Um eingehende Anfragen auf die Verwendung einer bestimmten Authentifizierungsmethode zu beschränken, können Sie diesen optionalen Bedingungsschlüssel verwenden. Sie können diesen Bedingungsschlüssel beispielsweise verwenden, um zuzulassen, dass nur der HTTP Authorization Header bei der Anforderungsauthentifizierung verwendet wird.</p> <p>Zulässige Werte:</p> <p>REST-HEADER</p> <p>REST-QUERY-STRING</p>
s3-outposts:signatureAge	<p>Die Zeitspanne in Millisekunden, die eine Signatur in einer authentifizierten Anfrage gültig ist.</p> <p>Diese Bedingung funktioniert nur für vorsignierte BenutzerURLs.</p> <p>In Signature Version 4 ist der Signierschlüssel bis zu sieben Tage lang gültig. Daher sind die Signaturen auch bis zu sieben Tage lang gültig. Weitere Informationen finden Sie unter Einführung in das Signieren von Anfragen in der Amazon Simple Storage API Service-Referenz. Sie können diese Bedingung verwenden, um das Alter der Unterschrift weiter einzuschränken.</p> <p>Beispielwert: 600000</p>
s3-outposts:x-amz-content-sha256	<p>Sie können diesen Bedingungsschlüssel verwenden, um nicht signierte Inhalte in Ihrem Bucket zu verbieten.</p> <p>Wenn Sie die Signature Version 4 verwenden, fügen Sie bei Anfragen, die den Authorization Header verwenden, den x-amz-content-sha256 Header in die Signaturberechnung ein und setzen dann seinen Wert auf die Hash-Nutzlast.</p>

Anwendbare Schlüssel	Beschreibung
	<p>Sie können diesen Bedingungsschlüssel in Ihrer Bucket-Richtlinie verwenden, um alle Uploads zu verweigern, deren Nutzdaten nicht signiert sind. Beispielsweise:</p> <ul style="list-style-type: none"> • Verweigern Sie Uploads, die den <code>Authorization</code> -Header zur Authentifizierung von Anfragen verwenden, aber die Nutzdaten nicht signieren. Weitere Informationen finden Sie unter Payload in einem einzigen Chunk übertragen in der Amazon Simple Storage Service API Reference. • Verweigern Sie Uploads, die vorsigniert verwenden. URLs Vorsignierte haben URLs immer eine. <code>UNSIGNED_PAYLOAD</code> Weitere Informationen finden Sie unter Authentifizieren von Anfragen und Authentifizierungsmethoden in der Amazon Simple Storage API Service-Referenz. <p>Zulässiger Wert: <code>UNSIGNED-PAYLOAD</code></p>

Beispiele für Bucket-Richtlinien, die mit der Signature Version 4 verbundene Bedingungsschlüssel verwenden

Um die folgenden Beispiele zu verwenden, ersetzen Sie das *Platzhalter für Benutzereingaben* mit Ihren eigenen Informationen.

Example : **s3-outposts:signatureAge**

Die folgende Bucket-Richtlinie lehnt alle vorsignierten URL Anfragen von S3 on Outposts für Objekte ab, `example-outpost-bucket` wenn die Signatur älter als 10 Minuten ist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Deny a presigned URL request if the signature is more than 10
minutes old",
      "Effect": "Deny",
      "Principal": {"AWS": "444455556666"},
    }
  ]
}
```

```

    "Action": "s3-outposts:*",
    "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/object/
**",
    "Condition": {
      "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
      "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
    }
  ]
}

```

Example : **s3-outposts:authType**

Die folgende Bucket-Richtlinie lässt nur Anfragen zu, die den Authorization-Header für die Anfrageauthentifizierung verwenden. Alle vorsignierten URL Anfragen werden abgelehnt, da vorsignierte Abfrageparameter zur Bereitstellung von Anfrage- und Authentifizierungsinformationen URLs verwenden. Weitere Informationen finden Sie unter [Authentifizierungsmethoden](#) in der Amazon Simple Storage Service API Reference.

```

{
  "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**

Die folgende Bucket-Richtlinie verweigert alle Uploads mit unsignierten Payloads, wie z. B. Uploads, die vorsignierte Payloads verwenden. URLs Weitere Informationen finden Sie unter [Authentifizieren von Anfragen](#) und [Authentifizierungsmethoden](#) in der Amazon Simple Storage API Service-Referenz.

```
{
  "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"
        }
      }
    }
  ]
}
```

AWS verwaltete Richtlinien für Amazon S3 auf Outposts

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet

ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien](#).

AWS verwaltete Richtlinie: AWSS3OnOutpostsServiceRolePolicy

Hilft Ihnen im Rahmen der serviceverknüpften Rolle `AWSServiceRoleForS3OnOutposts` bei der Verwaltung von Netzwerkressourcen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSS3OnOutpostsServiceRolePolicy](#).

S3 on Outposts aktualisiert AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für S3 auf Outposts an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen.

Änderung	Beschreibung	Datum
S3 on Outposts hat <code>AWSS3OnOutpostsServiceRolePolicy</code> hinzugefügt	S3 on Outposts hat <code>AWSS3OnOutpostsServiceRolePolicy</code> als Teil der serviceverknüpften Rolle <code>AWSServiceRoleForS3OnOutposts</code> hinzugefügt, die bei der Verwaltung von Netzwerkressourcen hilft.	3. Oktober 2023
S3 on Outposts hat mit der Verfolgung von Änderungen begonnen	S3 on Outposts hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien zu verfolgen.	3. Oktober 2023

Verwenden von serviceverknüpften Rollen für S3 on Outposts

Amazon S3 on Outposts verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte Rollen](#). Eine serviceverknüpfte Rolle ist ein einzigartiger IAM Rollentyp, der direkt mit S3 in Outposts

verknüpft ist. Dienstbezogene Rollen werden von S3 auf Outposts vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von S3 on Outposts, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. S3 on Outposts definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur S3 on Outposts die Rollen übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM Entität zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre S3-on-Outposts-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie unter [AWS Dienste, die mit Diensten funktionieren](#), IAM und suchen Sie in der Spalte mit dienstbezogenen Rollen nach den Diensten, für die Ja angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für S3 on Outposts

S3 on Outposts verwendet die benannte dienstverknüpfte Rolle, `AWSServiceRoleForS3OnOutposts` um Ihnen bei der Verwaltung von Netzwerkressourcen zu helfen.

Die serviceverknüpfte Rolle `AWSServiceRoleForS3OnOutposts` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `s3-outposts.amazonaws.com`

Die Rollenberechtigungsrichtlinie `AWSS3OnOutpostsServiceRolePolicy` ermöglicht S3 on Outposts die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

```
{
  "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"
}
]
```

Sie müssen Berechtigungen konfigurieren, damit eine IAM Entität (z. B. eine Rolle) eine dienstbezogene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Berechtigungen für dienstbezogene Rollen](#).

Erstellen einer serviceverknüpften Rolle für S3 on Outposts

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen S3-Endpunkt auf Outposts im AWS Management Console, dem oder dem erstellen AWS CLI, erstellt S3 on Outposts die AWS API serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen Endpunkt für S3 on Outposts erstellen, erstellt S3 on Outposts die serviceverknüpfte Rolle erneut für Sie.

Sie können die IAM Konsole auch verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall S3 on Outposts zu erstellen. Erstellen Sie im AWS CLI oder im AWS API eine dienstverknüpfte Rolle mit dem `s3-outposts.amazonaws.com` Dienstnamen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Erstellen einer dienstbezogenen Rolle](#). Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für S3 on Outposts

S3 on Outposts verhindert die Bearbeitung der `AWSServiceRoleForS3onOutposts` serviceverknüpften Rolle. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach der Erstellung nicht berücksichtigt werden. Sie können die Beschreibung der

Rolle jedoch mithilfe IAM von bearbeiten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Bearbeiten einer dienstbezogenen Rolle](#).

Löschen einer serviceverknüpften Rolle für S3 on Outposts

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Note

Wenn der S3-on-Outposts-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie S3 on Outposts-Ressourcen, die von der `AWSServiceRoleForS3OnOutposts` Rolle verwendet werden

1. [Löschen Sie die S3 on Outposts Endpoints](#) in Ihrem AWS-Konto Across all. AWS-Regionen
2. Löschen Sie die mit dem Service verknüpfte Rolle mithilfe von. IAM

Verwenden Sie die IAM Konsole, den oder AWS CLI, AWS API um die `AWSServiceRoleForS3OnOutposts` dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Löschen einer dienstbezogenen Rolle](#).

Unterstützte Regionen für serviceverknüpfte S3-on-Outposts-Rollen

S3 on Outposts unterstützt die Verwendung von dienstbezogenen Rollen überall dort, AWS-Regionen wo der Service verfügbar ist. Weitere Informationen finden Sie unter [S3-on-Outposts-Regionen und - Endpunkte](#).

Verwaltung von S3-on-Outposts-Speicher

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Weitere Informationen zum Verwalten und Freigeben Ihrer Speicherkapazität von Amazon S3 in Outposts finden Sie in den folgenden Themen.

Themen

- [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#)
- [Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket](#)
- [Replikation von Objekten für S3 in Outposts](#)
- [S3 auf Outposts teilen mit AWS RAM](#)
- [Andere AWS-Services , die S3 auf Outposts verwenden](#)

Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket

Wenn diese Option aktiviert ist, speichert die S3-Versionsverwaltung mehrere unterschiedliche Kopien eines Objekts im selben Bucket. Sie können die S3-Versionsverwaltung verwenden, um sämtliche Versionen aller Objekte in Ihren Outposts-Buckets zu speichern, abzurufen oder wiederherzustellen. Mit der S3-Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Buckets von Amazon S3 on Outposts verfügen über drei Versionsverwaltungsstatus:

- **Unversioned (Nicht versioniert)** – Wenn Sie die S3-Versionsverwaltung für Ihren Bucket noch nie aktiviert oder ausgesetzt haben, ist er nicht versioniert und gibt keinen S3-Versionsverwaltungsstatus zurück. Weitere Informationen über das S3-Versioning finden Sie unter [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#).
- **Enabled (Aktiviert)** – Aktiviert die S3-Versionsverwaltung für die Objekte im Bucket. Alle Objekte, die dem Bucket hinzugefügt werden, erhalten eine eindeutige Versions-ID. Objekte, die zum Zeitpunkt der Aktivierung des Versioning bereits im Bucket vorhanden waren, haben die Versions-ID null. Wenn Sie diese (oder andere) Objekte mit anderen Operationen ändern, z. B. [PutObject](#) erhalten die neuen Objekte eine eindeutige Versions-ID.
- **Suspended (Ausgesetzt)** – Setzt die S3-Versionsverwaltung für die Objekte im Bucket aus. Alle Objekte, die dem Bucket hinzugefügt werden, nachdem die Versionsverwaltung ausgesetzt wurde, erhalten die Versions-ID null. Weitere Informationen finden Sie im Amazon S3 S3-Benutzerhandbuch unter [Hinzufügen von Objekten zu Buckets mit aktivierter Versionierung](#).

Nachdem Sie die S3-Versionsverwaltung für einen S3-on-Outposts-Bucket aktiviert haben, kann er nicht mehr auf einen nicht versionierten Status zurückgesetzt werden. Sie können die Versionsverwaltung jedoch aussetzen. Weitere Informationen über das S3-Versioning finden Sie unter [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#).

Sie haben für jedes Objekt in Ihrem Bucket eine aktuelle Version und keine oder mehr vorherige Versionen. Damit die Speicherkosten gesenkt werden, können Sie die S3-Lebenszyklusregeln für Ihren Bucket so konfigurieren, dass vorherige Versionen nach einem bestimmten Zeitraum ablaufen. Weitere Informationen finden Sie unter [Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket](#).

Die folgenden Beispiele zeigen Ihnen, wie Sie die Versionierung für einen vorhandenen S3 on Outposts-Bucket mithilfe von AWS Management Console und AWS Command Line Interface (AWS CLI) aktivieren oder aussetzen können. Informationen zum Erstellen eines Buckets mit aktivierter S3-Versionsverwaltung finden Sie unter [Erstellen eines S3-on-Outposts-Buckets](#).

Note

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der Aktionen für ihn ausführen kann. Buckets verfügen über Konfigurationseigenschaften wie Outpost, Tags, Standard-Verschlüsselung und Zugriffspunkteinstellungen. Zu den Zugriffspunkteinstellungen gehören die virtuelle private Cloud (VPC), die

Zugriffspunktrichtlinie für den Zugriff auf die Objekte im Bucket und andere Metadaten.
Weitere Informationen finden Sie unter [Spezifikationen für S3 auf Outposts](#).

Verwenden der S3-Konsole

So bearbeiten Sie die S3-Versionsverwaltungseinstellungen für Ihren Bucket

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, für den Sie die S3-Versionsverwaltung aktivieren möchten.
4. Wählen Sie die Registerkarte Eigenschaften aus.
5. Wählen Sie unter Bucket Versioning (Bucket-Versioning) die Option Edit (Bearbeiten).
6. Bearbeiten Sie die S3-Versionsverwaltungseinstellung für den Bucket, indem Sie eine der folgenden Optionen auswählen:
 - Wenn Sie die S3-Versionsverwaltung aussetzen und die Erstellung neuer Objektversionen anhalten möchten, wählen Sie Suspend (Aussetzen) aus.
 - Möchten Sie die S3-Versionsverwaltung aktivieren und mehrere unterschiedliche Kopien jedes Objekts speichern, wählen Sie Enable (Aktivieren) aus.
7. Wählen Sie Änderungen speichern.

Verwenden Sie den AWS CLI

Um die S3-Versionierung für Ihren Bucket mithilfe von zu aktivieren oder zu unterbrechen AWS CLI, verwenden Sie den `put-bucket-versioning` Befehl, wie in den folgenden Beispielen gezeigt. Wenn Sie diese Beispiele verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

Weitere Informationen finden Sie [put-bucket-versioning](#) in der AWS CLI Referenz.

Example : S3-Versionsverwaltung aktivieren

```
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 : S3-Versionsverwaltung aussetzen

```
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
```

Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket

Sie können S3 Lifecycle verwenden, um die Speicherkapazität für Amazon S3 on Outposts zu optimieren. Sie können Lebenszyklusregeln erstellen, um Objekte ablaufen zu lassen, wenn sie veralten oder durch neuere Versionen ersetzt werden. Sie können eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen.

Weitere Informationen zum S3-Lebenszyklus finden Sie unter [Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket](#).

Note

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen kann.

Informationen zum Erstellen und Verwalten der Lebenszyklus-Konfiguration für Ihren S3-on-Outposts-Bucket finden Sie in den folgenden Themen.

Themen

- [Erstellen und Verwalten einer Lebenszyklusregel mithilfe der AWS Management Console](#)
- [Erstellen und Verwalten einer Lebenszykluskonfiguration mithilfe von AWS CLI und SDK für Java](#)

Erstellen und Verwalten einer Lebenszyklusregel mithilfe der AWS Management Console

Sie können S3 Lifecycle verwenden, um die Speicherkapazität für Amazon S3 on Outposts zu optimieren. Sie können Lebenszyklusregeln erstellen, um Objekte ablaufen zu lassen, wenn sie veralten oder durch neuere Versionen ersetzt werden. Sie können eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen.

Weitere Informationen zum S3-Lebenszyklus finden Sie unter [Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket](#).

Note

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen kann.

Informationen zum Erstellen und Verwalten einer Lebenszyklusregel für ein S3 auf Outposts mithilfe von finden Sie in den folgenden Themen. AWS Management Console

Themen


- [Erstellen einer Lebenszyklusregel](#)
- [Aktivieren einer Lebenszyklusregel](#)
- [Bearbeiten einer Lebenszyklusregel](#)
- [Löschen einer Lebenszyklusregel](#)

Erstellen einer Lebenszyklusregel

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, für den Sie eine Lebenszyklusregel erstellen möchten.
4. Wählen Sie die Registerkarte Management (Verwaltung) und dann die Option Create lifecycle rule (Lebenszyklusregel erstellen) aus.
5. Geben Sie einen Wert für Lifecycle rule name (Lebenszyklusregelname) ein.

6. Wählen Sie unter Rule scope (Regelumfang) eine der folgenden Optionen aus:
 - Wenn Sie den Umfang mit bestimmten Filtern einschränken möchten, wählen Sie Limit the scope of this rule using one or more filters (Geltungsbereich dieser Regel mit einem oder mehreren Filtern einschränken) aus. Fügen Sie anschließend einen Präfixfilter, Tags oder eine Objektgröße hinzu.
 - Wenn Sie diese Lebenszyklusregel auf alle Objekte im Bucket anwenden möchten, wählen Sie Apply to all objects in the bucket (Auf alle Objekte im Bucket anwenden) aus.
7. Wählen Sie unter Lifecycle rule actions (Lebenszyklusregelaktionen) eine der folgenden Optionen aus:
 - Expire current versions of objects (Aktuelle Objektversionen ablaufen lassen) – Bei Buckets mit aktivierter Versionsverwaltung fügt S3 on Outposts eine Löschmarkierung hinzu und behält die Objekte als nicht aktuelle Versionen bei. Bei Buckets, die keine S3-Versionsverwaltung verwenden, löscht S3 on Outposts die Objekte dauerhaft.
 - Permanently delete noncurrent versions of objects (Vorherige Objektversionen dauerhaft löschen) – S3 on Outposts löscht nicht aktuelle Objektversionen dauerhaft.
 - Delete expired object delete markers or incomplete multipart uploads (Abgelaufene Objektlöschmarkierungen oder unvollständige mehrteilige Uploads löschen) – S3 on Outposts löscht Löschmarkierungen für abgelaufene Objekte oder unvollständige mehrteilige Uploads dauerhaft.

Wenn Sie den Umfang Ihrer Lebenszyklusregel mithilfe von Objekt-Tags einschränken, können Sie die Option Delete expired object delete markers (Löschmarkierungen für abgelaufenes Objekt löschen) nicht auswählen. Sie können die Option Delete expired object delete markers (Löschmarkierungen für abgelaufenes Objekt löschen) auch nicht auswählen, wenn Sie Expire current object versions (Aktuelle Objektversionen ablaufen lassen) aktiviert haben.

 Note

Größenabhängige Filter können nicht mit Löschmarkierungen und unvollständigen mehrteiligen Uploads verwendet werden.

8. Wenn Sie Expire current versions of objects (Aktuelle Objektversionen ablaufen lassen) oder Permanently delete noncurrent versions of objects (Vorherige Objektversionen dauerhaft

- löschen) ausgewählt haben, konfigurieren Sie den Regelauslöser basierend auf einem bestimmten Datum oder dem Alter des Objekts.
9. Wenn Sie die Option Delete expired object delete markers (Löschmarkierungen für abgelaufenes Objekt löschen) ausgewählt haben, wählen Sie zur Bestätigung dieses Vorgangs die Option Delete expired object delete markers (Löschmarkierungen für abgelaufenes Objekt löschen) erneut aus.
 10. Überprüfen Sie unter Timeline Summary (Timeline-Zusammenfassung) Ihre Lebenszyklusregel und wählen Sie Create rule (Regel erstellen) aus.

Aktivieren einer Lebenszyklusregel

So aktivieren oder deaktivieren Sie eine Bucket-Lebenszyklusregel


1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, für den Sie eine Lebenszyklusregel deaktivieren möchten.
4. Wählen Sie die Registerkarte Management (Verwaltung) und dann unter Lifecycle rule (Lebenszyklusregel) die Regel aus, die Sie aktivieren oder deaktivieren möchten.
5. Wählen Sie für Aktion die Option Regel aktivieren oder deaktivieren aus.

Bearbeiten einer Lebenszyklusregel

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, für den Sie eine Lebenszyklusregel bearbeiten möchten.
4. Wählen Sie die Registerkarte Verwaltung und wählen Sie die Lebenszyklusregel aus, die Sie bearbeiten möchten.
5. (Optional) Aktualisieren Sie den Wert für Lifecycle rule name (Lebenszyklusregelname).
6. Bearbeiten Sie unter Rule scope (Regelumfang) den Umfang nach Bedarf:
 - Wenn Sie den Umfang mit bestimmten Filtern einschränken möchten, wählen Sie Limit the scope of this rule using one or more filters (Geltungsbereich dieser Regel mit einem oder mehreren Filtern einschränken) aus. Fügen Sie anschließend einen Präfixfilter, Tags oder eine Objektgröße hinzu.

- Wenn Sie diese Lebenszyklusregel auf alle Objekte im Bucket anwenden möchten, wählen Sie **Apply to all objects in the bucket** (Auf alle Objekte im Bucket anwenden) aus.
7. Wählen Sie unter **Lifecycle rule actions** (Lebenszyklusregelaktionen) eine der folgenden Optionen aus:
- **Expire current versions of objects** (Aktuelle Objektversionen ablaufen lassen) – Bei Buckets mit aktivierter Versionsverwaltung fügt S3 on Outposts eine Löschmarkierung hinzu und behält die Objekte als nicht aktuelle Versionen bei. Bei Buckets, die keine S3-Versionsverwaltung verwenden, löscht S3 on Outposts die Objekte dauerhaft.
 - **Permanently delete noncurrent versions of objects** (Vorherige Objektversionen dauerhaft löschen) – S3 on Outposts löscht nicht aktuelle Objektversionen dauerhaft.
 - **Delete expired object delete markers or incomplete multipart uploads** (Abgelaufene Objektlöschmarkierungen oder unvollständige mehrteilige Uploads löschen) – S3 on Outposts löscht Löschmarkierungen für abgelaufene Objekte oder unvollständige mehrteilige Uploads dauerhaft.

Wenn Sie den Umfang Ihrer Lebenszyklusregel mithilfe von Objekt-Tags einschränken, können Sie die Option **Delete expired object delete markers** (Löschmarkierungen für abgelaufenes Objekt löschen) nicht auswählen. Sie können die Option **Delete expired object delete markers** (Löschmarkierungen für abgelaufenes Objekt löschen) auch nicht auswählen, wenn Sie **Expire current object versions** (Aktuelle Objektversionen ablaufen lassen) aktiviert haben.

 Note

Größenabhängige Filter können nicht mit Löschmarkierungen und unvollständigen mehrteiligen Uploads verwendet werden.

8. Wenn Sie **Expire current versions of objects** (Aktuelle Objektversionen ablaufen lassen) oder **Permanently delete noncurrent versions of objects** (Vorherige Objektversionen dauerhaft löschen) ausgewählt haben, konfigurieren Sie den Regelauslöser basierend auf einem bestimmten Datum oder dem Objektalter.
9. Wenn Sie die Option **Delete expired object delete markers** (Löschmarkierungen für abgelaufenes Objekt löschen) ausgewählt haben, wählen Sie zur Bestätigung dieses Vorgangs die Option **Delete expired object delete markers** (Löschmarkierungen für abgelaufenes Objekt löschen) erneut aus.

10. Wählen Sie Save (Speichern) aus.

Löschen einer Lebenszyklusregel

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Outposts-Bucket aus, für den Sie eine Lebenszyklusregel löschen möchten.
4. Wählen Sie die Registerkarte Management (Verwaltung) und unter Lifecycle rule (Lebenszyklusregel) die Regel aus, die Sie löschen möchten.
5. Wählen Sie Löschen.

Erstellen und Verwalten einer Lebenszykluskonfiguration mithilfe von AWS CLI und SDK für Java

Sie können S3 Lifecycle verwenden, um die Speicherkapazität für Amazon S3 on Outposts zu optimieren. Sie können Lebenszyklusregeln erstellen, um Objekte ablaufen zu lassen, wenn sie veralten oder durch neuere Versionen ersetzt werden. Sie können eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen.

Weitere Informationen zum S3-Lebenszyklus finden Sie unter [Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket](#).

Note

Derjenige AWS-Konto, der den Bucket erstellt, besitzt ihn und ist der einzige, der eine Lebenszyklusregel erstellen, aktivieren, deaktivieren oder löschen kann.

Informationen zum Erstellen und Verwalten einer Lebenszykluskonfiguration für einen S3 on Outposts-Bucket mithilfe von AWS Command Line Interface (AWS CLI) und dem AWS SDK for Java finden Sie in den folgenden Beispielen.

Themen

- [PUTeine Lebenszykluskonfiguration](#)
- [GETdie Lebenszykluskonfiguration in einem S3-Bucket auf Outposts](#)

PUTeine Lebenszykluskonfiguration

AWS CLI

Im folgenden AWS CLI Beispiel wird eine Lebenszykluskonfigurationsrichtlinie auf einen Outposts-Bucket angewendet. Diese Richtlinie gibt an, dass alle Objekte mit dem gekennzeichneten Präfix (*myprefix*) und Tags nach 10 Tagen ablaufen. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

1. Speichern Sie die Lebenszyklus-Konfigurationsrichtlinie in einer JSON Datei. In diesem Beispiel heißt die Datei `lifecycle1.json`.

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

2. Reichen Sie die JSON Datei als Teil des `put-bucket-lifecycle-configuration` CLI Befehls ein. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen zu diesem Befehl finden Sie [put-bucket-lifecycle-configuration](#) in der AWS CLI Referenz.

```
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

Das folgende Beispiel SDK für Java platziert eine Lebenszykluskonfiguration in einem Outposts-Bucket. Diese Lebenszykluskonfiguration gibt an, dass alle Objekte mit dem gekennzeichneten Präfix (*myprefix*) und Tags nach 10 Tagen ablaufen. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen. Weitere Informationen finden Sie [PutBucketLifecycleConfiguration](#) in der Amazon Simple Storage Service API Reference.

```
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 die Lebenszykluskonfiguration in einem S3-Bucket auf Outposts

AWS CLI

Im folgenden AWS CLI Beispiel wird eine Lebenszykluskonfiguration für einen Outposts-Bucket abgerufen. Zum Verwenden dieses Befehls ersetzen Sie *user input placeholder* durch Ihre eigenen Informationen. Weitere Informationen zu diesem Befehl finden Sie [get-bucket-lifecycle-configuration](#) in der AWS CLI Referenz.

```
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

Das folgende Beispiel SDK für Java ruft eine Lebenszykluskonfiguration für einen Outposts-Bucket ab. Weitere Informationen finden Sie [GetBucketLifecycleConfiguration](#) in der Amazon Simple Storage Service API Reference.

```
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());
}
```

Replikation von Objekten für S3 in Outposts

Wenn die S3-Replikation aktiviert ist AWS Outposts, können Sie Amazon S3 on Outposts so konfigurieren, dass S3-Objekte automatisch zwischen verschiedenen Outposts oder zwischen Buckets auf demselben Outpost repliziert werden. Sie können S3 Replication in Outposts verwenden, um mehrere Replikate Ihrer Daten in denselben oder verschiedenen Outposts oder über verschiedene Konten hinweg zu verwalten und die Anforderungen an die Datenspeicherorte zu erfüllen. S3 Replication in Outposts hilft Ihnen dabei, Ihre Anforderungen an konforme Speicher und die Datenfreigabe zwischen verschiedenen Konten zu erfüllen. Wenn Sie sicherstellen müssen, dass Ihre Replikate mit den Quelldaten identisch sind, können Sie S3 Replication on Outposts verwenden, um Replikate Ihrer Objekte zu erstellen, die alle Metadaten wie Erstellungszeit, Tags und Version des ursprünglichen Objekts beibehalten. IDs

S3 Replication in Outposts stellt außerdem detaillierte Metriken und Benachrichtigungen zum Überwachen des Status der Objektreplication zwischen Buckets bereit. Sie können Amazon CloudWatch , um den Replikationsfortschritt zu überwachen, indem Sie die zur Replikation anstehenden Bytes, zur Replikation anstehende Vorgänge und die Replikationslatenz zwischen Ihren Quell- und Ziel-Buckets verfolgen. Um Konfigurationsprobleme schnell zu diagnostizieren und zu korrigieren, können Sie Amazon auch so einrichten, EventBridge dass es Benachrichtigungen über Fehler bei Replikationsobjekten erhält. Weitere Informationen hierzu finden Sie unter [Verwalten Ihrer Replikation](#).

Themen

- [Replikationskonfiguration](#)
- [Anforderungen für S3 Replication in Outposts](#)
- [Was wird repliziert?](#)

- [Was wird nicht repliziert?](#)
- [Was wird von S3 Replication in Outposts nicht unterstützt?](#)
- [Einrichten der Replikation](#)
- [Verwalten Ihrer Replikation](#)

Replikationskonfiguration

S3 on Outposts speichert eine Replikationskonfiguration als XML. In der XML Replikationskonfigurationsdatei geben Sie eine Rolle AWS Identity and Access Management (IAM) und eine oder mehrere Regeln an.

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

S3 in Outposts kann Objekte nur dann replizieren, wenn Sie die entsprechende Berechtigung erteilen. Sie gewähren S3 on Outposts Berechtigungen mit der IAM Rolle, die Sie in der Replikationskonfiguration angeben. S3 on Outposts übernimmt diese IAM Rolle, um Objekte in Ihrem Namen zu replizieren. Sie müssen der IAM Rolle die erforderlichen Berechtigungen erteilen, bevor Sie mit der Replikation beginnen. Weitere Informationen zu diesen Berechtigungen für S3 in Outposts finden Sie unter [Eine IAM Rolle erstellen](#).

In den folgenden Szenarien fügen Sie eine Regel zur Replikationskonfiguration hinzu:

- Sie möchten alle Objekte replizieren.
- Sie möchten eine Teilmenge der Objekte replizieren. Sie identifizieren die Teilmenge der Objekte, indem Sie einen Filter zur Regel hinzufügen. In dem Filter geben Sie ein Objektschlüsselpräfix, Markierungen oder eine Kombination aus beidem an, um die Objektmenge zu identifizieren, für die die Regel gilt.

Sie fügen mehrere Regeln zu einer Replikationskonfiguration hinzu, wenn Sie eine andere Teilmenge von Objekten replizieren möchten. In jeder Regel geben Sie einen Filter an, der eine andere Teilmenge von Objekten auswählt. Beispiel: Sie möchten Objekte mit dem Schlüsselpräfix `tax/` oder `document/` replizieren. Dazu fügen Sie zwei Regeln hinzu, eine, die den `tax/`-Schlüsselpräfix-Filter angibt und eine andere, die das `document/`-Schlüsselpräfix angibt.

Weitere Informationen zur Replikationskonfiguration und zu den Replikationsregeln von S3 on Outposts finden Sie [ReplicationConfiguration](#) in der Amazon Simple Storage Service API Reference.

Anforderungen für S3 Replication in Outposts

Für die Replikation ist Folgendes erforderlich:

- Der CIDR Outpost-Zielbereich muss in Ihrer Outpost-Subnetztabelle der Quelldatei zugeordnet sein. Weitere Informationen finden Sie unter [Voraussetzungen für das Erstellen von Konfigurationsregeln](#).
- Für Quell- und Ziel-Buckets muss die S3-Versionsverwaltung aktiviert sein. Weitere Informationen über das Versioning finden Sie unter [Verwalten der S3-Versionsverwaltung für Ihren S3-on-Outposts-Bucket](#).
- Amazon S3 in Outposts muss über die Berechtigung verfügen, Objekte aus dem Quell-Bucket in Ihrem Namen in den Ziel-Bucket zu replizieren. Dies bedeutet, dass Sie eine Servicerolle zum Delegieren von GET- und PUT-Berechtigungen an S3 in Outposts erstellen müssen.
 1. Bevor Sie die Servicerolle erstellen, benötigen Sie die GET-Berechtigung für den Quell-Bucket und die PUT-Berechtigung für den Ziel-Bucket.
 2. Um die Servicerolle zum Delegieren von Berechtigungen an S3 auf Outposts zu erstellen, müssen Sie zunächst Berechtigungen konfigurieren, damit eine IAM Entität (ein Benutzer oder eine Rolle) die Aktionen `iam:CreateRole` und `iam:PassRole` ausführen kann. Anschließend gestatten Sie der IAM Entität, eine Servicerolle zu erstellen. Damit S3 in Outposts die Servicerolle in Ihrem Namen annehmen kann und um GET- und PUT-Berechtigungen an S3 in Outposts zu delegieren, müssen Sie der Rolle die erforderlichen Vertrauens- und Berechtigungsrichtlinien zuordnen. Weitere Informationen zu diesen Berechtigungen für S3 in Outposts finden Sie unter [Eine IAM Rolle erstellen](#). Weitere Informationen zum Erstellen einer Servicerolle finden Sie unter [Erstellen einer Servicerolle](#).

Was wird repliziert?

Standardmäßig repliziert S3 in Outposts Folgendes:

- Objekte, die nach dem Hinzufügen einer Replikations-Konfiguration erstellt wurden.
- Objektmetadaten von den Quellobjekten zu den Replikaten Informationen zum Replizieren von Metadaten aus den Replikaten zu den Quellobjekten finden Sie unter [Replikationsstatus, wenn die Synchronisierung von Amazon-S3-Replikatänderungen in Outposts aktiviert ist](#).
- Objekt-Markierungen, sofern vorhanden.

Auswirkungen von Löschvorgänge auf die Replikation

Wenn Sie ein Objekt aus dem Quell-Bucket löschen, werden standardmäßig die folgenden Aktionen ausgeführt:

- Wenn Sie eine DELETE-Anforderung ohne Angabe einer Objektversions-ID stellen, fügt S3 in Outposts eine Löschmarkierung hinzu. S3 in Outposts geht wie folgt mit der Löschmarkierung um:
 - S3 in Outposts repliziert die Löschmarkierung standardmäßig nicht.
 - Sie können den non-tag-based Regeln jedoch die Replikation von Löschmarken hinzufügen. Weitere Informationen zum Aktivieren der Löschmarkierungs-Replikation in Ihrer Replikations-Konfiguration finden Sie unter [Verwenden der S3-Konsole](#).
- Wenn Sie in einer DELETE-Anforderung eine zu löschende Objektversions-ID angeben, löscht S3 in Outposts diese Objektversion im Quell-Bucket dauerhaft. Die Löschung wird jedoch nicht in den Ziel-Buckets repliziert. Anders ausgedrückt: Dieselbe Objektversion wird aus den Ziel-Buckets nicht gelöscht. Dieses Verhalten schützt Daten vor böswilligen Löschungen.

Was wird nicht repliziert?

Standardmäßig repliziert S3 in Outposts Folgendes nicht:

- Objekte im Quell-Bucket, bei denen es sich um Replikate handelt, die von einer anderen Replikationsregel erstellt wurden. Zum Beispiel: Angenommen Sie konfigurieren eine Replikation, bei der Bucket A die Quelle und Bucket B das Ziel ist. Nehmen wir jetzt an, Sie fügen eine weitere Replikations-Konfiguration hinzu, bei der Bucket B die Quelle und Bucket C das Ziel ist. In diesem Fall werden Objekte in Bucket B, die Replikate von Objekten in Bucket A sind, nicht in Bucket C repliziert.
- Objekte im Quell-Bucket, die bereits auf ein anderes Ziel repliziert wurden. Wenn Sie beispielsweise den Ziel-Bucket in einer vorhandenen Replikations-Konfiguration ändern, repliziert S3 in Outposts diese Objekte nicht erneut.

- Objekte, die mit serverseitiger Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C) erstellt wurden.
- Aktualisierungen von Unterressourcen auf Bucket-Ebene.

Wenn Sie beispielsweise die Lebenszyklus-Konfiguration ändern oder eine Benachrichtigungskonfiguration zu Ihrem Quell-Bucket hinzufügen, werden diese Änderungen nicht auf den Ziel-Bucket angewendet. Durch diese Funktion ist es möglich, für den Quell- und den Ziel-Bucket verschiedene Konfigurationen zu nutzen.

- Aktionen, die von der Lebenszyklus-Konfiguration durchgeführt werden.

Wenn Sie beispielsweise eine Lebenszykluskonfiguration nur auf Ihrem Quell-Bucket aktivieren und Ablaufaktionen konfigurieren, erstellt S3 in Outposts Löschmarkierungen für abgelaufene Objekte im Quell-Bucket, repliziert diese Markierungen jedoch nicht in den Ziel-Bucket. Wenn Sie dieselbe Lebenszyklus-Konfiguration sowohl auf den Quell- als auch auf den Ziel-Bucket anwenden möchten, aktivieren Sie für beide Buckets dieselbe Lebenszyklus-Konfiguration. Weitere Informationen zur Lebenszyklus-Konfiguration finden Sie unter [Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket](#).

Was wird von S3 Replication in Outposts nicht unterstützt?

Die folgenden Funktionen von S3 Replication werden von S3 in Outposts derzeit nicht unterstützt:

- S3-Replikationszeitsteuerung (S3). RTC S3 RTC wird nicht unterstützt, da der Objektverkehr in S3 Replication on Outposts über Ihr lokales Netzwerk (das lokale Gateway) übertragen wird. Weitere Informationen zu lokalen Gateways finden Sie unter [Arbeiten mit dem lokalen Gateway](#) im Benutzerhandbuch zu AWS Outposts .
- S3 Replication für Batchvorgänge.

Einrichten der Replikation

Note

Objekte, die bereits vor dem Einrichten einer Replikationsregel in Ihrem Bucket vorhanden waren, werden nicht automatisch repliziert. Anders ausgedrückt: Amazon S3 in Outposts repliziert Objekte nicht rückwirkend. Um Objekte zu replizieren, die vor Ihrer Replikationskonfiguration erstellt wurden, können Sie den CopyObject API Vorgang verwenden, um sie in denselben Bucket zu kopieren. Nach dem Kopieren werden die

Objekte als „neue“ Objekte im Bucket angezeigt und es gilt die Replikationskonfiguration für diese Objekte. Weitere Hinweise zum Kopieren eines Objekts finden Sie unter [Kopieren eines Objekts in einem Amazon S3 on Outposts-Bucket mit dem AWS SDK for Java](#) und [CopyObject](#) in der Amazon Simple Storage Service API Reference.

Um die S3 Replication in Outposts zu aktivieren, fügen Sie Ihrem Quell-Outposts-Bucket eine Replikationsregel hinzu. Die Replikationsregel weist S3 in Outposts an, Objekte wie angegeben zu replizieren. In der Replikationsregel müssen Sie Folgendes angeben:

- Der Quell-Outposts-Bucket-Zugriffspunkt — Der Access Point Amazon Resource Name (ARN) oder der Access Point-Alias des Buckets, von dem aus S3 on Outposts die Objekte replizieren soll. Weitere Informationen zur Verwendung von Zugriffspunktaliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-in-Outposts-Buckets](#).
- Die Objekte, die Sie replizieren möchten – Sie können alle Objekte im Quell-Outposts-Bucket replizieren oder nur eine Teilmenge davon. Teilmengen identifizieren Sie, indem Sie ein [Schlüsselnamenpräfix](#), mindestens ein Objekt-Tag oder beides in der Konfiguration angeben.

Wenn Sie beispielsweise eine Replikationsregel konfigurieren, um nur Objekte mit dem Schlüsselnamenpräfix `Tax/` zu replizieren, repliziert S3 in Outposts Objekte mit Schlüsseln wie `Tax/doc1` oder `Tax/doc2`. Es repliziert aber keine Objekte mit dem Schlüssel `Legal/doc3`. Wenn Sie sowohl ein Präfix als auch mindestens ein Tag angeben, repliziert S3 in Outposts nur Objekte, die dieses Schlüsselpräfix und diese Tags aufweisen.

- Der Ziel-Outposts-Bucket — Der ARN oder Access Point-Alias des Buckets, in den S3 on Outposts die Objekte replizieren soll.

Sie können die Replikationsregel mithilfe der RESTAPI, AWS SDKs, AWS Command Line Interface (AWS CLI) oder Amazon S3 S3-Konsole konfigurieren.

S3 on Outposts bietet auch API Operationen zur Unterstützung der Einrichtung von Replikationsregeln. Weitere Informationen finden Sie unter den folgenden Themen in der Amazon Simple Storage Service API Reference:

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

Themen

- [Voraussetzungen für das Erstellen von Konfigurationsregeln](#)
- [Erstellen von Replikationsregeln in Outposts](#)

Voraussetzungen für das Erstellen von Konfigurationsregeln

Themen

- [Verbinden Ihrer Quell- und Ziel-Outpost-Subnetze](#)
- [Eine IAM Rolle erstellen](#)

Verbinden Ihrer Quell- und Ziel-Outpost-Subnetze

Damit Ihr Replikationsdatenverkehr über Ihr lokales Gateway von Ihrem Quell-Outpost zu Ihrem Ziel-Outpost geleitet wird, müssen Sie eine neue Route hinzufügen, um das Netzwerk einzurichten. Sie müssen die Classless Inter-Domain Routing (CIDR) -Netzwerkbereiche Ihrer Access Points miteinander verbinden. Für jedes Zugriffspunktpaar müssen Sie diese Verbindung nur einmal einrichten.

Einige Schritte zum Einrichten der Verbindung unterscheiden sich je nach Zugriffstyp Ihrer Outposts-Endpunkte, die Ihren Zugriffspunkten zugeordnet sind. Der Zugriffstyp für Endgeräte ist entweder Privat (direktes Virtual Private Cloud [VPC] Routing für AWS Outposts) oder Kundeneigene IP (ein kundeneigener IP-Adresspool [CoIP-Pool] innerhalb Ihres lokalen Netzwerks).

Schritt 1: Finden Sie den CIDR Bereich Ihres Ausgangs-Outposts-Endpunkts

Um den CIDR Bereich Ihres Quellendpunkts zu ermitteln, der mit Ihrem Quell-Access-Point verknüpft ist

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie in der Liste Outposts-Buckets den gewünschten Quell-Bucket für die Replikation aus.
4. Wählen Sie die Registerkarte Outposts-Zugriffspunkte und anschließend den Outposts-Zugriffspunkt für den Quell-Bucket für Ihre Replikationsregel aus.
5. Wählen Sie den Outposts-Endpunkt aus.
6. Kopieren Sie die Subnetz-ID, die in [Schritt 5](#) verwendet werden soll.

7. Die Methode, mit der Sie den CIDR Bereich des Outposts-Quellendpunkts ermitteln, hängt vom Zugriffstyp Ihres Endpunkts ab.

Prüfen Sie im Abschnitt Outposts-Endpunkt – Übersicht den Zugriffstyp.

- [Wenn der Zugriffstyp Privat ist, kopieren Sie den Wert Classless Interdomain Routing \(CIDR\), der in Schritt 6 verwendet werden soll.](#)
- Wenn der Zugriffstyp Kundeneigene IP-Adresse lautet, gehen Sie wie folgt vor:
 1. Kopieren Sie den Wert „Kundeneigener IPv4 Pool“, um ihn später als ID für den Adresspool zu verwenden.
 2. Öffnen Sie die AWS Outposts Konsole unter <https://console.aws.amazon.com/outposts/>.
 3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabellen aus.
 4. Wählen Sie den Wert für Lokale Gateway-Routing-Tabellen-ID Ihres Quell-Outposts aus.
 5. Wählen Sie im Detailbereich die Registerkarte CoIP-Pools aus. Fügen Sie den Wert Ihrer CoIP-Pool-ID, den Sie zuvor kopiert haben, in das Suchfeld ein.
 6. Kopieren Sie für den passenden CoIP-Pool den entsprechenden CIDRsWert Ihres Quell-Outposts-Endpunkts zur Verwendung in [Schritt 6](#).

Schritt 2: Finden Sie die Subnetz-ID und den CIDR Bereich Ihres Outposts-Zielendpunkts

Um die Subnetz-ID und den CIDR Bereich Ihres Zielendpunkts zu ermitteln, der mit Ihrem Ziel-Access-Point verknüpft ist, folgen Sie denselben Teilschritten in [Schritt 1](#) und ändern Sie Ihren Outposts-Quellendpunkt in Ihren Outposts-Zielendpunkt, wenn Sie diese Unterschritte anwenden. Kopieren Sie den Subnetz-ID-Wert Ihres Ziel-Outposts-Endpunkts, um ihn in [Schritt 6](#) zu verwenden. Kopieren Sie den CIDR Wert Ihres Ziel-Outposts-Endpunkts zur Verwendung in [Schritt 5](#).

Schritt 3: Ermitteln der lokalen Gateway-ID Ihres Quell-Outposts

So ermitteln Sie die lokale Gateway-ID Ihres Quell-Outposts

1. Öffnen Sie die AWS Outposts Konsole unter <https://console.aws.amazon.com/outposts/>
2. Wählen Sie im linken Navigationsbereich Lokale Gateways aus.
3. Suchen Sie auf der Seite Lokale Gateways nach der Outpost-ID Ihres Quell-Outposts, den Sie für die Replikation verwenden möchten.
4. Kopieren Sie den Wert der lokalen Gateway-ID Ihres Quell-Outposts, um ihn in [Schritt 5](#) zu verwenden.

Weitere Informationen zu lokalen Gateways finden Sie unter [Lokales Gateway](#) im AWS Outposts - Benutzerhandbuch.

Schritt 4: Ermitteln der lokalen Gateway-ID Ihres Ziel-Outposts

Um die lokale Gateway-ID Ihres Ziel-Outposts zu ermitteln, führen Sie dieselben Unterschritte in [Schritt 3](#) aus, wobei Sie allerdings nach der Outpost-ID für Ihren Ziel-Outpost suchen. Kopieren Sie den Wert der lokalen Gateway-ID Ihres Ziel-Outposts, um ihn in [Schritt 6](#) zu verwenden.

Schritt 5: Einrichten der Verbindung von Ihrem Quell-Outpost-Subnetz zu Ihrem Ziel-Outpost-Subnetz

So richten Sie eine Verbindung von Ihrem Quell-Outpost-Subnetz zu Ihrem Ziel-Outpost-Subnetz ein

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die VPC Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Subnets aus.
3. Geben Sie im Suchfeld die Subnetz-ID für Ihren Quell-Outposts-Endpunkt ein, den Sie in [Schritt 1](#) ermittelt haben. Wählen Sie das Subnetz mit der übereinstimmenden Subnetz-ID aus.
4. Wählen Sie für das übereinstimmende Subnetzelement den Wert für Routing-Tabelle dieses Subnetzes aus.
5. Wählen Sie auf der Seite mit ausgewählter Routing-Tabelle Aktionen und dann Routen bearbeiten aus.
6. Wählen Sie auf der Seite Routen bearbeiten die Option Route hinzufügen aus.
7. Geben Sie unter Ziel den CIDR Bereich Ihres Ziel-Outposts-Endpunkts ein, den Sie in [Schritt 2](#) gefunden haben.
8. Wählen Sie unter Ziel Outpost lokales Gateway aus und geben Sie die lokale Gateway-ID Ihres Quell-Outposts ein, die Sie in [Schritt 3](#) ermittelt haben.
9. Wählen Sie Änderungen speichern.
10. Vergewissern Sie sich, dass der Status für die Route Aktiv lautet.

Schritt 6: Einrichten der Verbindung von Ihrem Ziel-Outpost-Subnetz zu Ihrem Quell-Outpost-Subnetz

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die VPC Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Subnets aus.

3. Geben Sie im Suchfeld die Subnetz-ID für Ihren Ziel-Outposts-Endpunkt ein, den Sie in [Schritt 2](#) ermittelt haben. Wählen Sie das Subnetz mit der übereinstimmenden Subnetz-ID aus.
4. Wählen Sie für das übereinstimmende Subnetzelement den Wert für Routing-Tabelle dieses Subnetzes aus.
5. Wählen Sie auf der Seite mit ausgewählter Routing-Tabelle Aktionen und dann Routen bearbeiten aus.
6. Wählen Sie auf der Seite Routen bearbeiten die Option Route hinzufügen aus.
7. Geben Sie unter Ziel den CIDR Bereich Ihres Ausgangs-Outposts-Endpunkts ein, den Sie in [Schritt 1](#) gefunden haben.
8. Wählen Sie unter Ziel Outpost lokales Gateway aus und geben Sie die lokale Gateway-ID Ihres Ziel-Outposts ein, die Sie in [Schritt 4](#) ermittelt haben.
9. Wählen Sie Änderungen speichern aus.
10. Vergewissern Sie sich, dass der Status für die Route Aktiv lautet.

Nachdem Sie die CIDR Netzwerkbereiche Ihrer Quell- und Zielzugriffspunkte verbunden haben, müssen Sie eine Rolle AWS Identity and Access Management (IAM) erstellen.

Eine IAM Rolle erstellen

Standardmäßig sind alle S3-in-Outputs-Ressourcen – Buckets, Objekte und zugehörige Unterressourcen – privat, sodass nur der Ressourcenbesitzer auf die Ressource zugreifen kann. S3 in Outputs benötigt Berechtigungen zum Lesen und Replizieren von Objekten aus dem Quell-Outposts-Bucket. Sie gewähren diese Berechtigungen, indem Sie eine IAM Servicerolle erstellen und diese Rolle in Ihrer Replikationskonfiguration angeben.

In diesem Abschnitt werden die Vertrauensrichtlinie und die mindestens erforderliche Berechtigungsrichtlinie erläutert. Die exemplarischen Vorgehensweisen enthalten step-by-step Anweisungen zum Erstellen einer IAM Rolle. Weitere Informationen finden Sie unter [Erstellen von Replikationsregeln in Outposts](#). Weitere Informationen zu IAM Rollen finden Sie im IAMBenutzerhandbuch unter [IAMRollen](#).

- Im folgenden Beispiel ist eine Vertrauensrichtlinie zu sehen, bei der Sie S3 in Outposts als Service-Prinzipal identifizieren, der die Rolle übernehmen kann.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3-outposts.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

- Im folgenden Beispiel wird eine Zugriffsrichtlinie gezeigt, bei der Sie der Rolle die Berechtigungen erteilen, Replikationsaufgaben in Ihrem Namen durchzuführen. Wenn S3 in Outposts die Rolle annimmt, verfügt es über die Berechtigungen, die Sie in dieser Richtlinie angeben. Wenn Sie diese Richtlinie verwenden möchten, ersetzen Sie *user input placeholders* durch eigene Informationen. Stellen Sie sicher, dass Sie sie durch den Outpost IDs Ihrer Quell- und Ziel-Outposts sowie die Bucket-Namen und Access Point-Namen Ihrer Quell- und Ziel-Outposts-Buckets ersetzen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET/object/*",
        "arn:aws:s3-outposts:region: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:region:123456789012:outpost/DESTINATION-OUTPOST-ID/
bucket/DESTINATION-OUTPOSTS-BUCKET/object/*",
        "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-OUTPOST-ID/
accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
    ]
}
]
```

Die Zugriffsrichtlinie erteilt Berechtigungen für folgenden Aktionen:

- `s3-outposts:GetObjectVersionForReplication` – Die Berechtigung für diese Aktion wird für alle Objekte erteilt, damit S3 in Outposts eine bestimmte Objektversion abrufen kann, die jedem Objekt zugeordnet ist.
- `s3-outposts:GetObjectVersionTagging`— Erlaubnis für diese Aktion für Objekte in *SOURCE-OUTPOSTS-BUCKET* Bucket (der Quell-Bucket) ermöglicht es S3 auf Outposts, Objekt-Tags für die Replikation zu lesen. Weitere Informationen finden Sie unter [Hinzufügen von Tags für S3-on-Outposts-Buckets](#). Wenn S3 in Outposts nicht über diese Berechtigung verfügt, repliziert es die Objekte, nicht jedoch die Objekt-Tags.
- `s3-outposts:ReplicateObject` und `s3-outposts:ReplicateDelete` — Berechtigungen für diese Aktionen für alle Objekte in *DESTINATION-OUTPOSTS-BUCKET* Bucket (der Ziel-Bucket) ermöglicht es S3 auf Outposts, Objekte zu replizieren oder Markierungen im Ziel-Outposts-Bucket zu löschen. Informationen zu Löschmarkierungen finden Sie unter [Auswirkungen von Löschvorgängen auf die Replikation](#).

Note

- Erlaubnis für die Aktion auf dem `s3-outposts:ReplicateObject` *DESTINATION-OUTPOSTS-BUCKET* Bucket (der Ziel-Bucket) ermöglicht auch die Replikation von Objekt-Tags. Daher müssen Sie für die `s3-outposts:ReplicateTags`-Aktion keine explizite Berechtigung erteilen.
- Für die kontoübergreifende Replikation muss der Besitzer des Outposts-Ziel-Buckets seine Bucket-Richtlinie aktualisieren, um die Erlaubnis für die `s3-outposts:ReplicateObject` Aktion auf dem *DESTINATION-OUTPOSTS-BUCKET*. Die `s3-outposts:ReplicateObject` Aktion ermöglicht es S3 on Outposts, Objekte und Objekt-Tags in den Outposts-Ziel-Bucket zu replizieren.

Eine Liste der Aktionen von S3 in Outposts finden Sie unter [Aktionen, die von Amazon S3 in Outposts definiert werden](#).

⚠ Important

Derjenige, dem die IAM Rolle gehört AWS-Konto, muss über Berechtigungen für die Aktionen verfügen, die er der Rolle gewährt. IAM

Angenommen, der Quell-Outposts-Bucket enthält Objekte, die im Besitz eines anderen AWS-Kontos sind. Der Eigentümer der Objekte muss demjenigen AWS-Konto, dem die IAM Rolle gehört, über die Bucket-Richtlinie und die Zugriffspunktrichtlinie ausdrücklich die erforderlichen Berechtigungen gewähren. Andernfalls kann S3 in Outposts nicht auf die Objekte zugreifen und die Replikation der Objekte schlägt fehl.

Die hier beschriebenen Berechtigungen gehören zur Mindest-Replikationskonfiguration. Wenn Sie optionale Replikationskonfigurationen hinzufügen möchten, müssen Sie S3 in Outposts zusätzliche Berechtigungen erteilen.

Erteilen von Berechtigungen, wenn die Quell- und Ziel-Outposts-Buckets unterschiedlichen Besitzern gehören AWS-Konten

Wenn sich die Quell- und Ziel-Outposts-Buckets nicht im Besitz desselben Kontos befinden, muss der Eigentümer des Ziel-Outposts-Buckets die Bucket- und Zugriffspunkt-Richtlinien für den Ziel-Bucket aktualisieren. Diese Richtlinien müssen dem Besitzer des Outposts-Quell-Buckets und der IAM Servicerolle die Berechtigungen zur Durchführung von Replikationsaktionen gewähren, wie in den folgenden Richtlinienbeispielen gezeigt. Andernfalls schlägt die Replikation fehl. In diesen Richtlinienbeispielen **DESTINATION-OUTPOSTS-BUCKET** ist der Ziel-Bucket. Wenn Sie diese Richtlinienbeispiele verwenden möchten, ersetzen Sie die *user input placeholders* durch Ihre Informationen.

Wenn Sie die IAM Servicerolle manuell erstellen, legen Sie den Rollenpfad auf `festrole/service-role/`, wie in den folgenden Richtlinienbeispielen gezeigt. Weitere Informationen finden Sie [IAMARNs](#) im IAMBenutzerhandbuch.

```
{
  "Version": "2012-10-17",
  "Id": "PolicyForDestinationBucket",
  "Statement": [
    {
```

```

        "Sid": "Permissions on objects",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::SourceBucket-account-ID:role/service-role/source-
account-IAM-role"
        },
        "Action": [
            "s3-outposts:ReplicateDelete",
            "s3-outposts:ReplicateObject"
        ],
        "Resource": [
            "arn:aws:s3-outposts:region:DestinationBucket-account-
ID:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET/object/*"
        ]
    }
]
}

```

```

{
  "Version": "2012-10-17",
  "Id": "PolicyForDestinationAccessPoint",
  "Statement": [
    {
      "Sid": "Permissions on objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::SourceBucket-account-ID:role/service-role/source-
account-IAM-role"
      },
      "Action": [
        "s3-outposts:ReplicateDelete",
        "s3-outposts:ReplicateObject"
      ],
      "Resource" : [
        "arn:aws:s3-outposts:region:DestinationBucket-account-
ID:outpost/DESTINATION-OUTPOST-ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/
object/*"
      ]
    }
  ]
}

```

Note

Wenn Objekte im Quell-Outposts-Bucket mit einem Tag versehen sind, beachten Sie Folgendes:

Wenn der Besitzer des Quell-Outposts-Buckets S3 on Outposts die Erlaubnis für die `s3-outposts:GetObjectVersionTagging` und `s3-outposts:ReplicateTags` Aktionen zur Replikation von Objekt-Tags (über die IAM Rolle) erteilt, repliziert Amazon S3 die Tags zusammen mit den Objekten. Informationen zur Rolle finden Sie unter IAM [Eine IAM Rolle erstellen](#)

Erstellen von Replikationsregeln in Outposts

S3-Replikation auf Outposts ist die automatische, asynchrone Replikation von Objekten über Buckets in demselben oder unterschiedlichen Buckets. AWS Outposts Bei der Replikation werden neu erstellte Objekte und Objektaktualisierungen aus einem Quell-Outposts-Bucket in einen oder mehrere Ziel-Outposts-Bucket(s) kopiert. Weitere Informationen finden Sie unter [Replikation von Objekten für S3 in Outposts](#).

Note

Objekte, die bereits vor dem Einrichten von Replikationsregeln in Ihrem Quell-Outposts-Bucket vorhanden waren, werden nicht repliziert. Anders ausgedrückt: S3 in Outposts repliziert Objekte nicht rückwirkend. Um Objekte zu replizieren, die vor Ihrer Replikationskonfiguration erstellt wurden, können Sie diese `CopyObject` API Operation verwenden, um sie in denselben Bucket zu kopieren. Nach dem Kopieren werden die Objekte als „neue“ Objekte im Bucket angezeigt und es gilt die Replikationskonfiguration für diese Objekte. Weitere Hinweise zum Kopieren eines Objekts finden Sie unter [Kopieren eines Objekts in einem Amazon S3 on Outposts-Bucket mit dem AWS SDK for Java](#) und [CopyObject](#) in der Amazon Simple Storage Service API Reference.

Wenn Sie die Replikation konfigurieren, fügen Sie dem Quell-Outposts-Bucket Replikationsregeln hinzu. Replikationsregeln definieren, welche Quell-Outposts-Bucket-Objekte repliziert werden sollen und in welchem Ziel-Outposts-Bucket/welchen Ziel-Outposts-Buckets die replizierten Objekte gespeichert werden sollen. Sie können eine Regel erstellen, um alle Objekte in einem Bucket oder eine Untermenge von Objekten mit einem spezifischen Schlüsselnamenpräfixen, einem oder

mehreren Objekt-Markierungen oder beidem zu replizieren. Ein Ziel-Outposts-Bucket kann sich in demselben Outpost wie der Quell-Outposts-Bucket oder in einem anderen Outpost befinden.

Für die Replikationsregeln von S3 on Outposts müssen Sie sowohl den Access Point Amazon Resource Name (ARN) des Quell-Outposts-Buckets als auch den Access Point des Ziel-Outposts-Buckets ARN anstelle der Quell- und Ziel-Outposts-Bucket-Namen angeben.

Wenn Sie angeben, dass eine Objektversions-ID gelöscht werden soll, löscht S3 in Outposts diese Objektversion im Quell-Outposts-Bucket. Die Löschung wird jedoch nicht in den Ziel-Outposts-Bucket repliziert. Anders ausgedrückt: Dieselbe Objektversion wird nicht aus dem Ziel-Outposts-Bucket gelöscht. Dieses Verhalten schützt Daten vor böswilligen Löschungen.

Wenn Sie einem Outposts-Bucket eine Replikationsregel hinzufügen, ist diese standardmäßig aktiviert, sodass sie ausgeführt wird, sobald Sie sie speichern.

In diesem Beispiel richten Sie eine Replikation für Quell- und Ziel-Outposts-Buckets ein, die sich in unterschiedlichen Outposts befinden und demselben AWS-Konto gehören. Es werden Beispiele für die Verwendung der Amazon S3 S3-Konsole, der AWS Command Line Interface (AWS CLI) und der AWS SDK for Java und bereitgestellt AWS SDK for .NET. Informationen zu den kontoübergreifenden Berechtigungen für die S3-Replikation in Outposts finden Sie unter [Erteilen von Berechtigungen, wenn die Quell- und Ziel-Outposts-Buckets unterschiedlichen Besitzern gehören AWS-Konten](#).

Die Voraussetzungen für die Einrichtung der Replikationsregeln von S3 in Outposts finden Sie unter [Voraussetzungen für das Erstellen von Konfigurationsregeln](#).

Verwenden der S3-Konsole

Führen Sie die folgenden Schritte aus, um eine Replikationsregel zu konfigurieren, wenn sich der Amazon-S3-in-Outposts-Ziel-Bucket in einem anderen Outpost als der Quell-Outposts-Bucket befindet.

Wenn sich der Ziel-Outposts-Bucket in einem anderen Konto als der Quell-Outposts-Bucket befindet, müssen Sie dem Ziel-Outposts-Bucket eine Bucket-Richtlinie hinzufügen, um dem Eigentümer des Quell-Outposts-Bucket-Kontos die Berechtigung zum Replizieren von Objekten in den Ziel-Outposts-Bucket zu erteilen.

So erstellen Sie eine Replikationsrolle

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.

2. Wählen Sie in der Liste Outposts-Buckets den Namen des Buckets aus, den Sie als Quell-Bucket verwenden möchten.
3. Wählen Sie die Registerkarte Verwaltung aus, scrollen Sie nach unten zum Abschnitt Replikationsregeln und wählen Sie dann Replikationsregel erstellen aus.
4. Geben Sie in Name der Replikationsregel einen Namen für Ihre Regel ein, um sie später besser identifizieren zu können. Der Name ist erforderlich und muss innerhalb des Buckets eindeutig sein.
5. In Status ist standardmäßig Aktiviert ausgewählt. Eine aktivierte Regel wird ausgeführt, sobald Sie speichern. Wenn Sie die Regel später aktivieren möchten, wählen Sie Deaktiviert aus.
6. Unter Priorität bestimmt der Prioritätswert der Regel, welche Regel im Falle einer Überschneidung von Regeln angewendet wird. Wenn Objekte in den Geltungsbereich von mehr als einer Replikationsregel fallen, verwendet S3 in Outposts diese Prioritätswerte, um Konflikte zu vermeiden. Standardmäßig werden neue Regeln mit der höchsten Priorität zur Replikationskonfiguration hinzugefügt. Je höher die Zahl, desto höher die Priorität.

Um die Priorität für die Regel zu ändern, wählen Sie nach dem Speichern der Regel zunächst den Namen der Regel aus der Liste der Replikationsregeln, dann Aktionen und schließlich Priorität bearbeiten aus.


7. Unter Quell-Bucket stehen Ihnen folgende Optionen zum Festlegen der Replikationsquelle zur Verfügung:
 - Um den gesamten Bucket zu replizieren, wählen Sie Auf alle Objekte im Bucket anwenden aus.
 - Um die Präfix- oder Tag-Filterung auf die Replikationsquelle anzuwenden, wählen Sie Geltungsbereich dieser Regel durch Verwendung von einem oder mehreren Filtern beschränken aus. Sie können ein Präfix und Markierungen kombinieren.
 - Um alle Objekte mit demselben Präfix zu replizieren, geben Sie unter Präfix ein Präfix in das Feld ein. Bei Verwendung des Filters Präfix ist die Replikation auf alle Objekte beschränkt, deren Namen mit derselben Zeichenfolge beginnen (z. B. `pictures`).

Wenn Sie ein Präfix eingeben, bei dem es sich um den Namen eines Ordners handelt, müssen Sie einen / (Schrägstrich) als letztes Zeichen eingeben (z. B. `pictures/`).

- Um alle Objekte mit einem oder mehreren gleichen Objekt-Tags zu replizieren, wählen Sie Tag hinzufügen aus und geben Sie das Schlüssel-Wert-Paar in die Felder ein. Wiederholen Sie den Vorgang, um ein weiteres Tag hinzuzufügen. Weitere Informationen über Objekt-Markierungen finden Sie unter [Hinzufügen von Tags für S3-on-Outposts-Buckets](#).

8. Um für die Replikation auf Ihren S3-in-Outposts-Quell-Bucket zuzugreifen, wählen Sie unter Quellzugriffspunktname einen Zugriffspunkt aus, der an den Quell-Bucket angehängt ist.
9. Wählen Sie unter Destination den Access Point ARN des Ziel-Outposts-Buckets aus, an dem S3 on Outposts Objekte replizieren soll. Der Ziel-Outposts-Bucket kann sich im selben oder einem anderen Bucket AWS-Konto wie der Quell-Outposts-Bucket befinden.

Wenn sich der Ziel-Bucket in einem anderen Konto als der Quell-Outposts-Bucket befindet, müssen Sie dem Ziel-Outposts-Bucket eine Bucket-Richtlinie hinzufügen, um dem Eigentümer des Quell-Outposts-Bucket-Kontos die Berechtigung zum Replizieren von Objekten in den Ziel-Outposts-Bucket zu erteilen. Weitere Informationen finden Sie unter [Erteilen von Berechtigungen, wenn die Quell- und Ziel-Outposts-Buckets unterschiedlichen Besitzern gehören AWS-Konten](#).

 Note

Wenn die Versionsverwaltung für den Ziel-Outposts-Bucket nicht aktiviert ist, erhalten Sie eine Warnmeldung, die die Schaltfläche Versionierung aktivieren enthält. Wählen Sie diese Schaltfläche, um das Versioning für den Bucket zu aktivieren.

10. Richten Sie eine AWS Identity and Access Management (IAM) -Servicerolle ein, die S3 on Outposts übernehmen kann, um Objekte in Ihrem Namen zu replizieren.

Um eine IAM Rolle einzurichten, führen Sie unter IAMRolle einen der folgenden Schritte aus:

- Damit S3 on Outposts eine neue IAM Rolle für Ihre Replikationskonfiguration erstellt, wählen Sie Aus vorhandenen IAM Rollen auswählen und dann Neue Rolle erstellen aus. Wenn Sie die Regel speichern, wird eine neue Richtlinie für die IAM Rolle generiert, die den von Ihnen ausgewählten Quell- und Ziel-Outposts-Buckets entspricht. Wir empfehlen Ihnen, die Option Neue Rolle erstellen auszuwählen.
- Sie können sich auch dafür entscheiden, eine bestehende IAM Rolle zu verwenden. In diesem Fall müssen Sie eine Rolle auswählen, die S3 in Outposts die erforderlichen Berechtigungen für die Replikation gewährt. Wenn diese Rolle S3 in Outposts keine ausreichenden Berechtigungen gewährt, um Ihre Replikationsregel zu befolgen, schlägt die Replikation fehl.

Um eine bestehende Rolle auszuwählen, wählen Sie Aus vorhandenen IAM Rollen auswählen und wählen Sie dann die Rolle aus dem Dropdownmenü aus. Sie können auch „IAMRolle eingeben“ wählen ARN und dann den Amazon-Ressourcennamen der IAM Rolle (ARN) eingeben.

⚠ Important

Wenn Sie eine Replikationsregel zu einem S3 on Outposts-Bucket hinzufügen, benötigen Sie die `iam:PassRole` Berechtigungen `iam:CreateRole` und, um die IAM Rolle erstellen und weitergeben zu können, die S3 on Outposts Replikationsberechtigungen gewährt. Weitere Informationen finden Sie im Benutzerhandbuch unter [Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle AWS-Service](#) an einen IAM

11. Alle Objekte in Outposts-Buckets sind standardmäßig verschlüsselt. Weitere Informationen zur Verschlüsselung in S3 in Outposts finden Sie unter [Datenverschlüsselung in S3 on Outposts](#). Nur Objekte, die mit serverseitiger Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln (SSE-S3) verschlüsselt wurden, können repliziert werden. Die Replikation von Objekten, die mit serverseitiger Verschlüsselung mit AWS Key Management Service (AWS KMS) - Schlüsseln (SSE-KMS) oder serverseitiger Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C) verschlüsselt wurden, wird nicht unterstützt.
12. Aktivieren Sie beim Festlegen der Konfiguration der Replikationsregeln nach Bedarf die folgenden zusätzlichen Optionen:
 - Wenn Sie S3-in-Outposts-Replikationsmetriken in Ihrer Replikationskonfiguration aktivieren möchten, wählen Sie Replikationsmetriken aus. Weitere Informationen finden Sie unter [Überwachen des Fortschritts mit Replikationsmetriken](#).
 - Wenn Sie die Löschkennzeichnung-Replikation in Ihrer Replikations-Konfiguration aktivieren möchten, wählen Sie Kennzeichnungreplikation löschen aus. Weitere Informationen finden Sie unter [Auswirkungen von Löschvorgängen auf die Replikation](#).
 - Wenn Sie an den Replikaten vorgenommene Metadatenänderungen zurück in die Quellobjekte replizieren möchten, wählen Sie Synchronisierung von Replikatänderungen aus. Weitere Informationen finden Sie unter [Replikationsstatus, wenn die Synchronisierung von Amazon-S3-Replikatänderungen in Outposts aktiviert ist](#).
13. Wählen Sie Regel erstellen aus, um den Vorgang abzuschließen.

Nach dem Speichern der Regel können Sie diese bearbeiten, aktivieren, deaktivieren oder löschen. Wechseln Sie hierfür auf die Registerkarte Verwaltung für den Quell-Outposts-Bucket, scrollen Sie nach unten zum Abschnitt Replikationsregeln, wählen Sie Ihre Regel aus und wählen Sie dann Regel bearbeiten aus.

Unter Verwendung der AWS CLI

Gehen Sie wie folgt vor AWS CLI , um die Replikation einzurichten, wenn die Quell- und Ziel-Outposts-Buckets demselben AWS-Konto gehören:

- Erstellen Sie Quell- und Ziel-Outposts-Buckets.
- Aktivieren Sie die Versionsverwaltung für beide Buckets.
- Erstellen Sie eine IAM Rolle, die S3 on Outposts die Erlaubnis erteilt, Objekte zu replizieren.
- Fügen Sie die Replikationskonfiguration zum Quell-Outposts-Bucket hinzu.

Um die Einrichtung zu prüfen, testen Sie sie.

Um die Replikation einzurichten, wenn die Quell- und Ziel-Outposts-Buckets demselben gehören AWS-Konto

1. Richten Sie das Anmeldeinformationsprofil für die AWS CLI ein. In diesem Beispiel verwenden wir den Profilnamen `acctA`. Informationen zum Einrichten der Anmeldeinformations-Profile finden Sie unter [Named Profiles](#) (Benannte Profile) im AWS Command Line Interface - Benutzerhandbuch.

Important

Das Profil, das Sie für diese Übung verwenden, muss über die nötigen Berechtigungen verfügen. In der Replikationskonfiguration geben Sie beispielsweise die IAM Servicerolle an, die S3 on Outposts übernehmen kann. Dies können Sie nur tun, wenn das verwendete Profil über die Berechtigungen `iam:CreateRole` und `iam:PassRole` verfügt. Weitere Informationen finden Sie im [Benutzerhandbuch unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle AWS-Service](#) an einen IAM Wenn Sie zur Erstellung eines benannten Profils die Anmeldeinformationen eines Administrators verwenden, verfügt das benannte Profil über die erforderliche Berechtigung, um alle Aufgaben durchzuführen.

2. Erstellen Sie einen *Quelle*-Bucket und aktivieren Sie das Versioning für ihn. Mit dem folgenden Befehl `create-bucket` wird ein *SOURCE-OUTPOSTS-BUCKET*-Bucket in der Region USA Ost (Nord-Virginia) (`us-east-1`) erstellt. Zur Verwendung dieses Befehls ersetzen Sie *user input placeholders* durch eigene Informationen.

```
aws s3control create-bucket --bucket SOURCE-OUTPOSTS-BUCKET --outpost-id SOURCE-OUTPOST-ID --profile acctA --region us-east-1
```

Mit dem folgenden Befehl `put-bucket-versioning` wird die Versionsverwaltung auf dem *SOURCE-OUTPOSTS-BUCKET*-Bucket aktiviert. Zur Verwendung dieses Befehls ersetzen Sie *user input placeholders* durch eigene Informationen.

```
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
```

- Erstellen Sie einen *Ziel*-Bucket und aktivieren Sie das Versioning für ihn. Mit dem folgenden Befehl `create-bucket` wird ein *DESTINATION-OUTPOSTS-BUCKET*-Bucket in der Region USA West (Oregon) (*us-west-2*) erstellt. Zur Verwendung dieses Befehls ersetzen Sie *user input placeholders* durch eigene Informationen.

Note

Um eine Replikationskonfiguration einzurichten, wenn sich sowohl der Quell- als auch der Ziel-Outposts-Bucket in demselben Namen befinden AWS-Konto, verwenden Sie dasselbe benannte Profil. Dieses Beispiel verwendet *acctA*. Um die Replikationskonfiguration zu testen, wenn die Buckets unterschiedlichen Besitzern gehören AWS-Konten, geben Sie für jeden Bucket unterschiedliche Profile an.

```
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
```

Mit dem folgenden Befehl `put-bucket-versioning` wird die Versionsverwaltung auf dem *DESTINATION-OUTPOSTS-BUCKET*-Bucket aktiviert. Zur Verwendung dieses Befehls ersetzen Sie *user input placeholders* durch eigene Informationen.

```
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. Erstellen Sie eine IAM Servicerolle. Zu einem späteren Zeitpunkt der Replikationskonfiguration fügen Sie diese Servicerolle dem *SOURCE-OUTPOSTS-BUCKET*-Bucket hinzu. S3 in Outposts übernimmt diese Rolle, um Objekte in Ihrem Namen zu replizieren. Sie erstellen eine IAM Rolle in zwei Schritten:
 - a. Erstellen Sie eine IAM Rolle.
 - i. Kopieren Sie die folgende Vertrauensrichtlinie und speichern Sie sie in einer Datei mit dem Namen `s3-on-outposts-role-trust-policy.json` im aktuellen Verzeichnis auf Ihrem lokalen Computer. Diese Richtlinie gewährt S3 in Outposts Service-Prinzipal-Berechtigungen, um die Servicerolle anzunehmen.

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

- ii. Führen Sie den folgenden -Befehl aus, um die Rolle zu erstellen. Ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
aws iam create-role --role-name replicationRole --assume-role-policy-document file://s3-on-outposts-role-trust-policy.json --profile acctA
```

- b. Fügen Sie eine Berechtigungsrichtlinie zur Servicerolle hinzu.
 - i. Kopieren Sie die folgende Berechtigungsrichtlinie und speichern Sie sie in einer Datei mit dem Namen `s3-on-outposts-role-permissions-policy.json` im aktuellen Verzeichnis auf Ihrem lokalen Computer. Diese Richtlinie erteilt Berechtigungen für verschiedene S3-in-Outposts-Bucket- und -Objektaktionen. Wenn Sie diese Richtlinie verwenden möchten, ersetzen Sie *user input placeholders* durch eigene Informationen.

```
{
```

```

"Version":"2012-10-17",
"Statement":[
  {
    "Effect":"Allow",
    "Action":[
      "s3-outposts:GetObjectVersionForReplication",
      "s3-outposts:GetObjectVersionTagging"
    ],
    "Resource":[
      "arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-
      OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET/object/*",
      "arn:aws:s3-outposts:region: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:region:123456789012:outpost/DESTINATION-
      OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET/object/*",
      "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-
      OUTPOST-ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
    ]
  }
]
}

```

- ii. Führen Sie den folgenden Befehl aus, um eine Richtlinie zu erstellen und sie der Rolle anzufügen. Ersetzen Sie *user input placeholders* durch Ihre Informationen.

```

aws iam put-role-policy --role-name replicationRole --policy-
document file://s3-on-outposts-role-permissions-policy.json --policy-
name replicationRolePolicy --profile acctA

```

5. Fügen Sie eine Replikationskonfiguration zum *SOURCE-OUTPOSTS-BUCKET*-Bucket hinzu.
 - a. Obwohl für S3 on Outposts API eine Replikationskonfiguration im XML Format AWS CLI erforderlich ist, müssen Sie die Replikationskonfiguration im JSON Format angeben. Speichern Sie Folgendes JSON in einer Datei namens `replication.json` im lokalen

Verzeichnis auf Ihrem Computer. Wenn Sie diese Konfiguration verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
{
  "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. Führen Sie den folgenden Befehl `put-bucket-replication` aus, um die Replikationskonfiguration zu Ihrem Quell-Outposts-Bucket hinzuzufügen. Zur Verwendung dieses Befehls ersetzen Sie *user input placeholders* durch eigene Informationen.

```
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. Um die Replikationskonfiguration abzurufen, verwenden Sie den Befehl `get-bucket-replication`. Zur Verwendung dieses Befehls ersetzen Sie *user input placeholders* durch eigene Informationen.

```
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. Testen Sie das Setup in der Amazon-S3-Konsole:

- a. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.

- b. Erstellen Sie im *SOURCE-OUTPOSTS-BUCKET*-Bucket einen Ordner mit dem Namen Tax.
- c. Fügen Sie Beispielobjekte zum Tax-Ordner im *SOURCE-OUTPOSTS-BUCKET*-Bucket hinzu.
- d. Überprüfen Sie im *DESTINATION-OUTPOSTS-BUCKET*-Bucket Folgendes:
 - S3 in Outposts hat die Objekte repliziert.

 Note

Die von S3 in Outposts für die Replikation eines Objekts benötigte Zeit hängt von der Größe des Objekts ab. Weitere Informationen zum Anzeigen des Replikationsstatus finden Sie unter [Abrufen von Replikationsstatusinformationen](#).

- Auf der Registerkarte Eigenschaften des Objekts ist Replikationsstatus auf Replikat gesetzt (sodass dies als Replikatobjekt identifiziert wird).

Verwalten Ihrer Replikation

In diesem Abschnitt werden zusätzliche Optionen für die Replikationskonfiguration beschrieben, die in S3 in Outposts verfügbar sind, und es wird erörtert, wie Sie den Replikationsstatus ermitteln und Replikationsprobleme beheben können. Weitere Informationen zum Erstellen einer grundlegenden Replikationskonfiguration finden Sie unter [Einrichten der Replikation](#).

Themen

- [Überwachen des Fortschritts mit Replikationsmetriken](#)
- [Abrufen von Replikationsstatusinformationen](#)
- [Fehlerbehebung bei einer Replikation](#)
- [EventBridge Für die S3-Replikation auf Outposts verwenden](#)

Überwachen des Fortschritts mit Replikationsmetriken

S3 Replication in Outposts bietet detaillierte Metriken für die Replikationsregeln in Ihrer Replikationskonfiguration. Mithilfe der Replikationsmetriken können Sie den Fortschritt der Replikation in 5-Minuten-Intervallen überwachen. Verfolgen Sie dazu die Bytes der ausstehenden Replikation, die Replikationslatenz und die Operationen mit ausstehender Replikation. Um Sie bei der Behebung von Konfigurationsproblemen zu unterstützen, können Sie Amazon auch so einrichten, EventBridge dass es Benachrichtigungen über Replikationsfehler erhält.

Wenn Replikationsmetriken aktiviert sind, veröffentlicht S3 Replication on Outposts die folgenden Metriken auf Amazon CloudWatch:

- Bytes der ausstehenden Replikation – Die Gesamtzahl der Bytes von Objekten, deren Replikation für eine bestimmte Replikationsregel aussteht.
- Replikationslatenz – Die maximale Anzahl von Sekunden, um die der Replikations-Ziel-Bucket für eine bestimmte Replikationsregel hinter dem Quell-Bucket zurückliegt.
- Operationen mit ausstehender Replikation – Die Anzahl der Operationen, deren Replikation für eine bestimmte Replikationsregel aussteht. Zu den Operationen gehören Objekte, Löschmarkierungen und Tags.

Note

Metriken zur S3-Replikation auf Outposts werden zum gleichen Tarif wie für CloudWatch benutzerdefinierte Metriken abgerechnet. [Weitere Informationen finden Sie unter CloudWatch Preise.](#)

Abrufen von Replikationsstatusinformationen

Der Replikationsstatus hilft Ihnen, den aktuellen Status eines Objekts zu bestimmen, das gerade von Amazon S3 in Outposts repliziert wird. Der Replikationsstatus eines Quellobjekts gibt entweder PENDING, COMPLETED oder FAILED zurück. Der Replikationsstatus eines Replikats gibt REPLICA zurück.

Übersicht über den Replikationsstatus

In einem Replikationsszenario haben Sie einen Quell-Bucket, auf dem Sie die Replikation konfigurieren, und einen Ziel-Bucket, in den S3 in Outposts Objekte repliziert. Wenn Sie ein Objekt (unter Verwendung von `GetObject`) oder Objektmetadaten (unter Verwendung von `HeadObject`) von diesen Buckets anfordern, gibt S3 in Outposts den Header `x-amz-replication-status` wie folgt in der Antwort zurück:

- Wenn Sie ein Objekt aus dem Quell-Bucket anfordern, gibt S3 in Outposts den Header `x-amz-replication-status` zurück, wenn das Objekt in der Anforderung für die Replikation geeignet ist.

Nehmen wir beispielsweise an, dass Sie in Ihrer Replikationskonfiguration das Objektpräfix `TaxDocs` angeben, um S3 in Outposts anzuweisen, nur Objekte mit dem Schlüsselnamenpräfix `TaxDocs` zu replizieren. Alle Objekte mit diesem Schlüsselnamenpräfix, die Sie hochladen, z. B. `TaxDocs/document1.pdf`, werden repliziert. Für Objektanforderungen mit diesem Schlüsselnamenpräfix gibt S3 in Outposts den Header `x-amz-replication-status` mit einem der folgenden Werte für den Replikationsstatus des Objekts zurück: `PENDING`, `COMPLETED` oder `FAILED`.

Note

Wenn nach dem Hochladen eines Objekts die Objektreplikation fehlschlägt, können Sie die fehlgeschlagene Replikation nicht erneut durchzuführen versuchen. Sie müssen das Objekt erneut hochladen. Bei Problemen wie fehlenden Replikationsrollen-Berechtigungen oder fehlenden Bucket-Berechtigungen gehen Objekte in den Status `FAILED` über. Bei temporären Fehlern, z. B. wenn ein Bucket oder Ihr Outpost nicht verfügbar ist, geht der Replikationsstatus nicht in `FAILED` über, sondern verbleibt bei `PENDING`. Wenn die Ressource wieder online ist, setzt S3 in Outposts die Replikation dieser Objekte fort.

- Wenn Sie ein Objekt aus einem Ziel-Bucket anfordern und es sich bei dem Objekt in Ihrer Anforderung um ein Replikat handelt, das von S3 in Outposts erstellt wurde, gibt S3 in Outposts den Header `x-amz-replication-status` mit dem Wert `REPLICA` zurück.

Note

Bevor Sie ein Objekt aus einem Quell-Bucket löschen, bei dem die Replikation aktiviert ist, sollten Sie den Replikationsstatus des Objekts überprüfen, um sicherzustellen, dass das Objekt repliziert wurde.

Replikationsstatus, wenn die Synchronisierung von Amazon-S3-Replikatänderungen in Outposts aktiviert ist

Wenn in Ihren Replikationsregeln die Synchronisierung von S3-in-Outposts-Replikatänderungen aktiviert ist, können Replikate einen anderen Status als `REPLICA` melden. Wenn Änderungen an Metadaten gerade repliziert werden, gibt der Header `x-amz-replication-status` für das Replikat `PENDING` zurück. Wenn bei der Synchronisierung der Replikatänderungen die Replikation

von Metadaten fehlschlägt, gibt der Header für das Replikat FAILED zurück. Wenn Metadaten korrekt repliziert werden, gibt der Header für das Replikat den Wert REPLICICA zurück.

Fehlerbehebung bei einer Replikation

Wenn Objektreplikate nicht im Amazon-S3-in-Outposts-Ziel-Bucket angezeigt werden, nachdem Sie die Replikation konfiguriert haben, können Sie mit diesen Tipps zur Fehlerbehebung Probleme identifizieren und beheben.

- Wie lange Amazon S3 in Outposts für die Replikation eines Objekts benötigt, hängt von verschiedenen Faktoren ab, unter anderem von der Distanz zwischen den Quell- und Ziel-Outposts und der Größe des Objekts.

Sie können den Replikationsstatus des Quellobjekts überprüfen. Wenn der Replikationsstatus des Objekts PENDING lautet, hat S3 in Outposts die Replikation noch nicht abgeschlossen. Wenn der Replikationsstatus des Objekts FAILED lautet, überprüfen Sie die Replikationskonfiguration des Quell-Buckets.

- Überprüfen Sie in der Replikations-Konfiguration des Quell-Buckets Folgendes:
 - Der Access Point Amazon Resource Name (ARN) des Ziel-Buckets ist korrekt.
 - ob das Schlüsselnamenpräfix korrekt ist. Wenn Sie beispielsweise die Konfiguration so einrichten, dass nur Objekte mit dem Präfix Tax repliziert werden, werden nur Objekte mit Schlüsselnamen wie beispielsweise Tax/document1 oder Tax/document2 repliziert. Ein Objekt mit dem Schlüsselnamen document3 wird nicht repliziert.
 - Der Status lautet Enabled.
- Stellen Sie sicher, dass die Versionsverwaltung bei keinem der beiden Buckets ausgesetzt wurde. Sowohl für die Quell- als auch für die Ziel-Buckets muss die Versionsverwaltung aktiviert sein.
- Wenn der Ziel-Bucket einem anderen gehört AWS-Konto, stellen Sie sicher, dass der Bucket-Besitzer eine Bucket-Richtlinie für den Ziel-Bucket hat, die es dem Besitzer des Quell-Buckets ermöglicht, Objekte zu replizieren. Ein Beispiel finden Sie unter [Erteilen von Berechtigungen, wenn die Quell- und Ziel-Outposts-Buckets unterschiedlichen Besitzern gehören AWS-Konten](#).
- Wenn ein Objektreplikat nicht im Ziel-Bucket angezeigt wird, könnte Folgendes die Replikation verhindern:
 - S3 in Outposts repliziert keine Objekte in einem Quell-Bucket, bei dem es sich um ein Replikat handelt, das mit einer anderen Replikationskonfiguration erstellt wurde. Wenn Sie beispielsweise ein Replikationskonfiguration von Bucket A zu Bucket B zu Bucket C festlegen, repliziert S3 in Outposts keine Objektreplikate in Bucket B zu Bucket C.

Wenn Sie Objekte in Bucket A zu Bucket B und Bucket C replizieren möchten, legen Sie mehrere Bucket-Ziele in unterschiedlichen Replikationsregeln für Ihre Quell-Bucket-Replikationskonfiguration fest. Erstellen Sie beispielsweise zwei Replikationsregeln für Quell-Bucket A, wobei eine Regel für die Replikation in Ziel-Bucket B und die andere Regel für die Replikation in Ziel-Bucket C gilt.

- Ein Quell-Bucket-Besitzer kann anderen Personen die AWS-Konten Berechtigung zum Hochladen von Objekten gewähren. Standardmäßig besitzt der Quell-Bucket-Eigentümer keine Berechtigungen für die Objekte, die von anderen Konten erstellt wurden. Die Replikations-Konfiguration repliziert nur die Objekte, für die der Quell-Bucket-Eigentümer über Zugriffsberechtigungen verfügt. Um Replikationsprobleme zu vermeiden, kann der Besitzer des Quell-Buckets andere AWS-Konten Berechtigungen zum Erstellen von Objekten unter bestimmten Bedingungen gewähren, was explizite Zugriffsberechtigungen für diese Objekte erfordert.
- Angenommen, Sie fügen einer Replikationskonfiguration eine Regel hinzu, um eine Teilmenge von Objekten mit einem spezifischen Tag zu replizieren. In diesem Fall müssen Sie den spezifischen Tag-Schlüssel und -Wert zum Zeitpunkt der Objekterstellung zuweisen, damit S3 in Outposts das Objekt replizieren kann. Wenn Sie zuerst ein Objekt erstellen und dann dem vorhandenen Objekt das Tag hinzufügen, repliziert S3 in Outposts das Objekt nicht.
- Die Replikation schlägt fehl, wenn die Bucket-Richtlinie den Zugriff auf die Replikationsrolle für eine der folgenden Aktionen verweigert:

Quell-Bucket

```
"s3-outposts:GetObjectVersionForReplication",  
"s3-outposts:GetObjectVersionTagging"
```

Ziel-Buckets:

```
"s3-outposts:ReplicateObject",  
"s3-outposts:ReplicateDelete",  
"s3-outposts:ReplicateTags"
```

- Amazon EventBridge kann Sie benachrichtigen, wenn Objekte nicht zu ihren Ziel-Außenposten repliziert werden. Weitere Informationen finden Sie unter [EventBridge Für die S3-Replikation auf Outposts verwenden](#).

EventBridge Für die S3-Replikation auf Outposts verwenden

Amazon S3 on Outposts ist in Amazon integriert EventBridge und verwendet den `s3-outposts` Namespace. EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. Weitere Informationen finden Sie unter [Was ist Amazon EventBridge?](#) im EventBridge Amazon-Benutzerhandbuch.

Um Sie bei der Behebung von Problemen mit der Replikationskonfiguration zu unterstützen, können Sie Amazon so einrichten EventBridge, dass es Benachrichtigungen über Replikationsfehler erhält. EventBridge kann Sie benachrichtigen, wenn Objekte nicht zu ihren Ziel-Außenposten repliziert werden. Weitere Informationen zum aktuellen Status eines zu replizierenden Objekts finden Sie unter [Übersicht über den Replikationsstatus](#).

Immer wenn bestimmte Ereignisse in Ihrem Outposts-Bucket passieren, kann S3 on Outposts Ereignisse an senden. EventBridge Anders als bei anderen Zielen müssen Sie nicht auswählen, welche Ereignistypen Sie liefern möchten. Sie können auch EventBridge Regeln verwenden, um Ereignisse an weitere Ziele weiterzuleiten. Nach EventBridge der Aktivierung sendet S3 on Outposts alle folgenden Ereignisse an EventBridge.

Ereignistyp	Beschreibung	Namespace
OperationFailedReplication	Die Replikation eines Objekts innerhalb einer Replikationsregel ist fehlgeschlagen. Weitere Informationen darüber, warum S3 Replication in Outposts fehlgeschlagen ist, finden Sie unter Wird verwendet EventBridge , um die S3-Replikation auf Outposts anzuzeigen: Fehlerursachen .	s3-outposts

Wird verwendet EventBridge , um die S3-Replikation auf Outposts anzuzeigen: Fehlerursachen

In der folgenden Tabelle sind Gründe für das Fehlschlagen von S3 Replication in Outposts aufgeführt. Sie können eine EventBridge Regel so konfigurieren, dass die Fehlerursache über Amazon Simple Queue Service (AmazonSQS), Amazon Simple Notification Service (AmazonSNS) oder Amazon CloudWatch Logs veröffentlicht und angezeigt wird. AWS Lambda Weitere Informationen zu den Berechtigungen, die für die Nutzung dieser Ressourcen erforderlich sind EventBridge, finden Sie unter [Verwenden ressourcenbasierter Richtlinien](#) für. EventBridge

Gründe für das Fehlschlagen der Replikation	Beschreibung
AssumeRoleNotPermitted	S3 on Outposts kann die Rolle AWS Identity and Access Management (IAM) nicht annehmen, die in der Replikationskonfiguration angegeben ist.
DstBucketNotFound	S3 in Outposts kann den in der Replikationskonfiguration angegebenen Ziel-Bucket nicht finden.
DstBucketUnversioned	Die Versionsverwaltung ist im Outposts-Ziel-Bucket nicht aktiviert. Um Objekte mit S3 Replication in Outposts replizieren zu können, müssen Sie die Versionsverwaltung im Ziel-Bucket aktivieren.
DstDelObjNotPermitted	S3 in Outposts kann Löschvorgänge nicht in den Ziel-Bucket replizieren. Möglicherweise fehlt die <code>s3-outposts:ReplicateDelete</code> -Berechtigung für den Ziel-Bucket.
DstMultipartCompleteNotPermitted	S3 in Outposts kann einen mehrteiligen Upload von Objekten in den Ziel-Bucket nicht abschließen. Möglicherweise fehlt die <code>s3-outposts:ReplicateObject</code> -Berechtigung für den Ziel-Bucket.
DstMultipartInitNotPermitted	S3 in Outposts kann einen mehrteiligen Upload von Objekten in den Ziel-Bucket nicht initiieren. Möglicherweise fehlt die <code>s3-outposts:ReplicateObject</code> -Berechtigung für den Ziel-Bucket.
DstMultipartPartUploadNotPermitted	S3 on Outposts kann keine mehrteiligen Upload-Objekte in den Ziel-Bucket hochladen. Möglicherweise fehlt die <code>s3-outpos</code>

Gründe für das Fehlschlagen der Replikation	Beschreibung
	<p><code>s3:ReplicateObject</code> -Berechtigung für den Ziel-Bucket.</p>
<p><code>DstOutOfCapacity</code></p>	<p>S3 in Outposts kann nicht in den Ziel-Outpost replizieren, da die S3-Speicherkapazität des Outposts aufgebraucht ist.</p>
<p><code>DstPutObjNotPermitted</code></p>	<p>S3 in Outposts kann keine Objekte in den Ziel-Bucket replizieren. Möglicherweise fehlt die <code>s3-outposts:ReplicateObject</code> -Berechtigung für den Ziel-Bucket.</p>
<p><code>DstPutTaggingNotPermitted</code></p>	<p>S3 in Outposts kann keine Objekt-Tags in den Ziel-Bucket replizieren. Möglicherweise fehlt die <code>s3-outposts:ReplicateObject</code> -Berechtigung für den Ziel-Bucket.</p>
<p><code>DstVersionNotFound</code></p>	<p>S3 in Outposts kann die Objektversion, die benötigt wird, um die Metadaten dieser Objektversion zu replizieren, nicht im Ziel-Bucket finden.</p>
<p><code>SrcBucketReplicationConfigMissing</code></p>	<p>S3 in Outposts kann keine Replikationskonfiguration für den Zugriffspunkt finden, der dem Quell-Outposts-Bucket zugeordnet ist.</p>
<p><code>SrcGetObjNotPermitted</code></p>	<p>S3 in Outposts kann nicht auf das Objekt im Quell-Bucket für die Replikation zugreifen. Möglicherweise fehlt die <code>s3-outposts:GetObjectVersionForReplication</code> -Berechtigung für den Quell-Bucket.</p>

Gründe für das Fehlschlagen der Replikation	Beschreibung
<code>SrcGetTaggingNotPermitted</code>	S3 in Outposts kann nicht auf Objekt-Tag-Informationen vom Quell-Bucket zugreifen . Möglicherweise fehlt die <code>s3-outposts:GetObjectVersionTagging</code> - Berechtigung für den Quell-Bucket.
<code>SrcHeadObjectNotPermitted</code>	S3 in Outposts kann keine Objektmetadaten aus dem Quell-Bucket abrufen. Möglicherweise fehlt die <code>s3-outposts:GetObjectVersionForReplication</code> -Berechtigung für den Quell-Bucket.
<code>SrcObjectNotEligible</code>	Das Objekt kann nicht repliziert werden. Das Objekt oder seine Objekt-Tags stimmt/stimmen nicht mit der Replikationskonfiguration überein.

Weitere Informationen zur Behebung von Replikationsfehlern finden Sie in folgenden Themen:

- [Eine IAM Rolle erstellen](#)
- [Fehlerbehebung bei einer Replikation](#)

Überwachung mit EventBridge CloudWatch

Für die Überwachung ist Amazon EventBridge in Amazon integriert CloudWatch. EventBridge sendet automatisch Metriken an CloudWatch jede Minute. Zu diesen Metriken gehören die Anzahl der [Ereignisse](#), die von einer [Regel](#) abgeglichen wurden, sowie die Anzahl der Aufrufe eines [Ziels](#) durch eine Regel. Wenn eine Regel ausgeführt wird EventBridge, werden alle mit der Regel verknüpften Ziele aufgerufen. Sie können Ihr EventBridge Verhalten auf folgende CloudWatch Weise überwachen.

- Sie können die verfügbaren [EventBridgeMetriken](#) für Ihre EventBridge Regeln vom CloudWatch Dashboard aus überwachen. Anschließend können Sie CloudWatch Funktionen wie CloudWatch Alarme verwenden, um Alarme für bestimmte Metriken einzurichten. Wenn diese Metriken die

benutzerdefinierten Schwellenwerte erreichen, die Sie in den Alarmen angegeben haben, erhalten Sie Benachrichtigungen und können entsprechende Maßnahmen ergreifen.

- Sie können Amazon CloudWatch Logs als Ziel Ihrer EventBridge Regel festlegen. EventBridge erstellt dann Protokollstreams und CloudWatch Logs speichert den Text der Ereignisse als Protokolleinträge. Weitere Informationen finden Sie unter [EventBridge und CloudWatch Protokolle](#).

Weitere Informationen zum Debuggen von EventBridge Ereignissen bei der Übertragung und Archivierung von Ereignissen finden Sie in den folgenden Themen:

- [Richtlinie zur Wiederholung von Ereignissen und Verwendung von Warteschlangen für unzustellbare Nachrichten](#)
- [Archivieren von Ereignissen EventBridge](#)

S3 auf Outposts teilen mit AWS RAM

Amazon S3 on Outposts unterstützt die gemeinsame Nutzung von S3-Kapazität für mehrere Konten innerhalb einer Organisation mithilfe von AWS Resource Access Manager ([AWS RAM](#)). Mit der Freigabe von S3 in Outposts können Sie anderen erlauben, Buckets, Endpunkte und Zugriffspunkte in Ihrem Outpost zu erstellen und zu verwalten.

In diesem Thema wird gezeigt, wie Sie AWS RAM S3 auf Outposts und verwandte Ressourcen mit anderen AWS-Konto in Ihrer AWS Organisation teilen können.

Voraussetzungen

- Für das Outpost-Eigentümerkonto ist eine Organisation in AWS Organizations konfiguriert. Weitere Informationen finden Sie unter [Erstellen einer Organisation](#) im Benutzerhandbuch für AWS Organizations .
- Die Organisation umfasst AWS-Konto die, mit der Sie Ihre S3 on Outposts-Kapazität teilen möchten. Weitere Informationen finden Sie unter [Senden von Einladungen an AWS-Konten](#) im Benutzerhandbuch für AWS Organizations .
- Wählen Sie eine der folgenden Optionen, die Sie freigeben möchten. Die zweite Ressource (entweder Subnets (Subnetze) oder Outposts) muss ausgewählt sein, damit auch Endpunkte zugänglich sind. Endpunkte sind eine Netzwerkanforderung, um auf Daten zuzugreifen, die in S3 in Outposts gespeichert sind.

Option 1	Option 2
<p>S3 in Outposts</p> <p>Erlaubt es dem Benutzer, Buckets auf Ihren Outposts und Zugriffspunkten zu erstellen und diesen Buckets Objekte hinzuzufügen.</p> <p>Subnets</p> <p>Ermöglicht dem Benutzer die Nutzung Ihrer virtuellen privaten Cloud (VPC) und der Endpunkte, die Ihrem Subnetz zugeordnet sind.</p>	<p>S3 in Outposts</p> <p>Erlaubt es dem Benutzer, Buckets auf Ihren Outposts und Zugriffspunkten zu erstellen und diesen Buckets Objekte hinzuzufügen.</p> <p>Outposts</p> <p>Erlaubt dem Benutzer das Anzeigen von S3-Kapazitätstabellen und der AWS Outposts -Konsolen-Startseite. Erlaubt es Benutzern außerdem, Subnetze auf freigegebenen Outposts zu erstellen und Endpunkte zu erstellen.</p>

Verfahren

1. [Melden Sie sich mit AWS Management Console dem an AWS-Konto , dem der Outpost gehört, und öffnen Sie dann die AWS RAM Konsole unter /ram. https://console.aws.amazon.com](https://console.aws.amazon.com/ram)
2. Vergewissern Sie sich, dass Sie das Teilen mit AWS Organizations in aktiviert haben. AWS RAM Weitere Informationen finden Sie unter [Freigabe für Ressourcen in AWS Organizations aktivieren](#) im AWS RAM -Benutzerhandbuch.
3. Verwenden Sie entweder Option 1 oder Option 2 in den [Voraussetzungen](#), um eine Ressourcenfreigabe zu erstellen. Wenn Sie über mehrere S3 on Outposts-Ressourcen verfügen, wählen Sie die Amazon-Ressourcennamen (ARNs) der Ressourcen aus, die Sie teilen möchten. Wenn Sie Endpunkte aktivieren möchten, teilen Sie entweder Ihr Subnetz oder Ihren Outpost.

Weitere Informationen zum Erstellen einer Ressourcenfreigabe finden Sie unter [Erstellen einer Ressourcenfreigabe](#) im AWS RAM -Benutzerhandbuch.

4. Die AWS-Konto Personen, mit denen Sie Ihre Ressourcen geteilt haben, sollten jetzt S3 auf Outposts verwenden können. Abhängig von der Option, die Sie in den [Voraussetzungen](#) gewählt haben, geben Sie dem Kontobenutzer die folgenden Informationen an:

Option 1	Option 2
Die Outpost-ID	Die Outpost-ID
Die VPC ID	
Die Subnetz-ID	
Die Sicherheitsgruppen-ID	

Note

Der Benutzer kann mithilfe der AWS RAM Konsole AWS Command Line Interface (AWS CLI), oder bestätigen, dass die Ressourcen für ihn freigegeben wurden RESTAPI. AWS SDKs Der Benutzer kann seine vorhandenen Ressourcenfreigaben mithilfe des [get-resource-shares](#)CLIBefehls einsehen.

Verwendungsbeispiele

Nachdem Sie Ihre S3 in Outposts-Ressourcen mit einem anderen Konto geteilt haben, kann dieses Konto Buckets und Objekte in Ihrem Outpost verwalten. Wenn Sie die Ressource Subnets (Subnetze) freigegeben haben, kann dieses Konto den von Ihnen erstellten Endpunkt verwenden. Die folgenden Beispiele zeigen, wie ein Benutzer den verwenden kann AWS CLI , um mit Ihrem Outpost zu interagieren, nachdem Sie diese Ressourcen gemeinsam genutzt haben.

Example : Erstellen eines Buckets

Im folgenden Beispiel wird ein Bucket mit dem Namen erstellt *amzn-s3-demo-bucket1* auf dem Outpost *op-01ac5d28a6a232904*. Bevor Sie diesen Befehl verwenden, ersetzen Sie jeden *user input placeholder* mit den entsprechenden Werten für Ihren Anwendungsfall.

```
aws s3control create-bucket --bucket amzn-s3-demo-bucket1 --outpost-  
id op-01ac5d28a6a232904
```

Weitere Informationen über diesen Befehl finden Sie unter [create-bucket](#) in der AWS CLI -Referenz.

Example : Erstellen eines Zugriffspunkts

Im folgenden Beispiel wird ein Zugriffspunkt in einem Outpost erstellt, wobei die Beispielparameter in der folgenden Tabelle verwendet werden. Bevor Sie diesen Befehl verwenden, ersetzen Sie diese *user input placeholder* Werte und den AWS-Region Code durch die entsprechenden Werte für Ihren Anwendungsfall.

Parameter	Wert
Konto-ID	<i>111122223333</i>
Name des Zugriffspunkts	<i>example-outpost-access-point</i>
Outpost-ID	<i>op-01ac5d28a6a232904</i>
Name des Outpost-Buckets	<i>amzn-s3-demo-bucket1</i>
VPCID	<i>vpc-1a2b3c4d5e6f7g8h9</i>

Note

Der Account-ID-Parameter muss die ID des Bucket-Besitzers sein, bei dem es sich um den gemeinsamen Benutzer handelt. AWS-Konto

```
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
```

Weitere Informationen zu diesem Befehl finden Sie [create-access-point](#) in der AWS CLI Referenz.

Example : Hochladen eines Objekts

Im folgenden Beispiel wird die Datei hochgeladen *my_image.jpg* vom lokalen Dateisystem des Benutzers zu einem Objekt mit dem Namen *images/my_image.jpg* durch den Access Point *example-outpost-access-point* auf dem Außenposten *op-01ac5d28a6a232904*, im Besitz des Accounts AWS *111122223333*. Bevor Sie diesen Befehl verwenden, ersetzen Sie diese *user*

input placeholder Werte und den AWS-Region Code durch die entsprechenden Werte für Ihren Anwendungsfall.

```
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
```

Weitere Informationen über diesen Befehl finden Sie unter [put-object](#) in der AWS CLI -Referenz.

Note

Wenn dieser Vorgang zu einem Fehler „Ressource nicht gefunden“ führt oder nicht reagiert, haben Sie VPC möglicherweise keinen gemeinsamen Endpunkt.

Verwenden Sie den [list-shared-endpoints](#) AWS CLI Befehl, um zu überprüfen, ob es einen gemeinsamen Endpunkt gibt. Wenn kein freigegebener Endpunkt vorhanden ist, erstellen Sie einen Endpunkt gemeinsam mit dem Outpost-Besitzer. Weitere Informationen finden Sie [ListSharedEndpoints](#) in der Amazon Simple Storage Service API Reference.

Example : Erstellen eines Endpunkts

Das folgende Beispiel erstellt einen Endpunkt für einen freigegebenen Outpost. Bevor Sie diesen Befehl verwenden, ersetzen Sie die *user input placeholder*-Werte für die Outpost-ID, die Subnetz-ID und die Sicherheitsgruppen-ID durch die entsprechenden Werte für Ihren Anwendungsfall.

Note

Der Benutzer kann diesen Vorgang nur ausführen, wenn die Ressourcenfreigabe die Outposts-Ressource enthält.

```
aws s3outposts create-endpoint --outposts-id op-01ac5d28a6a232904 --subnet-id XXXXXX --security-group-id XXXXXX
```

Weitere Informationen über diesen Befehl finden Sie unter [create-endpoint](#) in der AWS CLI -Referenz.

Andere AWS-Services , die S3 auf Outposts verwenden

Andere AWS-Services , die lokal bei Ihnen laufen, AWS Outposts können auch Ihre Amazon S3 on Outposts-Kapazität nutzen. In Amazon zeigt CloudWatch der S3Outposts Namespace detaillierte Metriken für Buckets innerhalb von S3 auf Outposts an, aber diese Metriken beinhalten nicht die Nutzung für andere. AWS-Services Informationen zur Verwaltung Ihrer S3 on Outposts-Kapazität, die von anderen verbraucht wird AWS-Services, finden Sie in der folgenden Tabelle.

AWS-Service	Beschreibung	Weitere Informationen
Amazon S3	Jede direkte Nutzung von S3 auf Outposts hat ein passendes Konto und eine passende CloudWatch Bucket-Metrik.	Siehe Metriken
Amazon Elastic Block Store (AmazonEBS)	Für Amazon EBS on Outposts können Sie einen AWS Outpost als Snapshot-Ziel wählen und ihn lokal in Ihrem S3 auf Outpost speichern.	Weitere Informationen
Amazon Relational Database Service (AmazonRDS)	Sie können RDS lokale Backups von Amazon verwenden , um Ihre RDS Backups lokal auf Ihrem Outpost zu speichern.	Weitere Informationen

Überwachen von S3 in Outposts

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Weitere Informationen zum Überwachen Ihrer Speicherkapazität von Amazon S3 in Outposts finden Sie in den folgenden Themen.

Themen

- [Verwaltung der Kapazität von S3 on Outposts mit Amazon-Metriken CloudWatch](#)
- [Empfangen von S3 on Outposts-Ereignisbenachrichtigungen mithilfe von Amazon CloudWatch Events](#)
- [Überwachen von S3 in Outposts mit Protokollen in AWS CloudTrail](#)

Verwaltung der Kapazität von S3 on Outposts mit Amazon-Metriken CloudWatch

Um die Verwaltung der festen S3-Kapazität in Ihrem Outpost zu erleichtern, empfehlen wir Ihnen, CloudWatch Warnmeldungen zu erstellen, die Sie darüber informieren, wenn Ihre Speichernutzung einen bestimmten Schwellenwert überschreitet. Weitere Informationen zu den CloudWatch Metriken für S3 auf Outposts finden Sie unter [CloudWatch Metriken](#). Wenn in Ihrem Outpost nicht genügend Speicherplatz zum Speichern eines Objekts vorhanden ist, wird eine Ausnahme für unzureichende Kapazität API zurückgegeben (ICE). Um Speicherplatz freizugeben, können Sie CloudWatch Alarme erstellen, die eine explizite Datenlöschung auslösen, oder eine Lebenszyklus-Ablaufrichtlinie verwenden, um Objekte ablaufen zu lassen. Um Daten vor dem Löschen zu speichern, können AWS DataSync Sie Daten aus Ihrem Amazon S3 on Outposts Bucket in einen S3-Bucket in einem AWS-

Region kopieren. Weitere Informationen zur Verwendung DataSync finden Sie unter [Erste Schritte mit AWS DataSync](#) im AWS DataSync Benutzerhandbuch.

CloudWatch Metriken

Der S3Outposts Namespace enthält die folgenden Metriken für Amazon S3 auf Outposts-Buckets. Sie können die Gesamtzahl der bereitgestellten S3 in Outposts-Bytes, die für Objekte insgesamt verfügbaren freien Bytes und die Gesamtgröße aller Objekte für einen bestimmten Bucket überwachen. Bucket- oder kontobezogene Metriken gibt es für die gesamte direkte S3-Nutzung. Die indirekte S3-Nutzung, wie das Speichern lokaler Snapshots von Amazon Elastic Block Store oder Backups von Amazon Relational Database Service auf einem Outpost, verbraucht S3-Kapazität, ist aber nicht in den Bucket- oder kontobezogenen Metriken enthalten. Weitere Informationen zu EBS lokalen Amazon-Snapshots finden Sie unter [EBS Lokale Amazon-Snapshots auf Outposts](#). Ihren EBS Amazon-Kostenbericht finden Sie unter <https://console.aws.amazon.com/billing/>.

Note

S3 in Outposts unterstützt nur die folgenden Metriken und keine anderen Amazon-S3-Metriken.

Da S3 on Outposts ein festes Kapazitätslimit hat, empfehlen wir, CloudWatch Alarme zu erstellen, um Sie zu benachrichtigen, wenn Ihre Speichernutzung einen bestimmten Schwellenwert überschreitet.

Metrik	Beschreibung	Zeitraum	Einheiten	Typ
OutpostTotalBytes	Die gesamte bereitgestellte Kapazität in Byte für einen Outpost	5 Minuten	Bytes	S3 on Outposts
OutpostFreeBytes	Die Anzahl der freien Bytes, die auf Outposts zum Speichern von Kundendaten verfügbar sind.	5 Minuten	Bytes	S3 on Outposts
BucketUsedBytes	Die Gesamtgröße aller Objekte für den angegebenen Bucket.	5 Minuten	Bytes	S3 on Outposts Nur direkte S3-Nutzung

Metrik	Beschreibung	Zeitraum	Einheiten	Typ
AccountTotalBytes	Die Gesamtgröße aller Objekte für das angegebene Outposts-Konto.	5 Minuten	Bytes	S3 on Outposts Nur direkte S3-Nutzung
BytesPerReplication	Die Gesamtanzahl der Bytes von Objekten, deren Replikation für eine bestimmte Replikationsregel aussteht. Weitere Informationen zum Aktivieren von Replikationsmetriken finden Sie unter Erstellen von Replikationsregeln zwischen Outposts .	5 Minuten	Bytes	Optional. Für S3 Replication in Outposts.
OperationsPending	Die Gesamtanzahl der Operationen, deren Replikation für eine bestimmte Replikationsregel aussteht. Weitere Informationen zum Aktivieren von Replikationsmetriken finden Sie unter Erstellen von Replikationsregeln zwischen Outposts .	5 Minuten	Zählungen	Optional. Für S3 Replication in Outposts.
ReplicationLatency	Die aktuelle Verzögerung in Sekunden, um die der Replikationsziel-Bucket hinter dem Quell-Bucket für eine bestimmte Replikationsregel zurückliegt. Weitere Informationen zum Aktivieren von Replikationsmetriken finden Sie unter Erstellen von Replikationsregeln zwischen Outposts .	5 Minuten	Sekunden	Optional. Für S3 Replication in Outposts.

Empfangen von S3 on Outposts-Ereignisbenachrichtigungen mithilfe von Amazon CloudWatch Events

Sie können CloudWatch Ereignisse verwenden, um eine Regel für jedes Amazon S3 on API Outposts-Ereignis zu erstellen. Wenn Sie eine Regel erstellen, können Sie wählen, ob Sie über alle unterstützten CloudWatch Ziele benachrichtigt werden möchten, einschließlich Amazon Simple Queue Service (AmazonSQS), Amazon Simple Notification Service (AmazonSNS) und AWS Lambda. Weitere Informationen finden Sie in der Liste der [AWS Dienste, die Ziele für CloudWatch Veranstaltungen sein können](#), im Amazon CloudWatch Events-Benutzerhandbuch. Informationen zur Auswahl eines Zieldienstes, der mit Ihrem S3 auf Outposts funktioniert, finden Sie im Amazon CloudWatch CloudWatch Events-Benutzerhandbuch [unter Erstellen einer Ereignisregel, die AWS CloudTrail bei einem AWS API Aufruf ausgelöst wird](#).

Note

Bei Objektoperationen in S3 on Outposts entsprechen die von gesendeten AWS API Anrufergebnisse nur CloudTrail dann Ihren Regeln, wenn Sie Trails (optional mit Event-Selektoren) für den Empfang dieser Ereignisse konfiguriert haben. Weitere Informationen finden Sie unter [Arbeiten mit CloudTrail Protokolldateien](#) im AWS CloudTrail Benutzerhandbuch.

Example

Es folgt eine Beispielregel für den DeleteObject-Vorgang. Zum Verwenden dieser Beispielregel ersetzen Sie *amzn-s3-demo-bucket1* durch den Namen Ihres S3-in-Outposts-Buckets.

```
{
  "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"
    ]
  }
}
```

Überwachen von S3 in Outposts mit Protokollen in AWS CloudTrail

Amazon S3 on Outposts ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in S3 auf Outposts ausgeführten Aktionen bereitstellt. Sie können mit AWS CloudTrail Informationen über Anforderungen auf Bucket- und Objektebene in S3 in Outposts abrufen, um Ihre S3-in-Outposts-Ereignisaktivitäten zu überprüfen und zu protokollieren.

Um CloudTrail Datenereignisse für alle Ihre Outposts-Buckets oder für eine Liste bestimmter Outposts-Buckets zu aktivieren, müssen Sie manuell [einen Trail in erstellen](#). CloudTrail Weitere Informationen zu CloudTrail Protokolldateieinträgen finden Sie unter Protokolldateieinträge von [S3 on Outposts](#).

Eine vollständige Liste der CloudTrail Datenereignisse für S3 auf Outposts finden Sie unter [Amazon S3 S3-Datenereignisse CloudTrail im](#) Amazon S3 S3-Benutzerhandbuch.

Note

- Es hat sich bewährt, eine Lebenszyklusrichtlinie für Ihren Outposts-Bucket für AWS CloudTrail Datenereignisse zu erstellen. Konfigurieren Sie die Lebenszyklusrichtlinie zum regelmäßigen Entfernen von Protokolldateien nach dem Zeitraum, der für die Überprüfung erforderlich ist. Dadurch wird die Menge der Daten reduziert, die Amazon Athena in einer Abfrage analysiert. Weitere Informationen finden Sie unter [Erstellen und Verwalten einer Lebenszyklus-Konfiguration für Ihren Amazon-S3-on-Outposts-Bucket](#).
- Beispiele für das Abfragen von CloudTrail Protokollen finden Sie im AWS Big-Data-Blogbeitrag [Analyze Security, Compliance, and Operational Activity Using AWS CloudTrail and Amazon Athena](#).

Aktivieren CloudTrail Sie die Protokollierung für Objekte in einem S3-Bucket auf Outposts

Sie können die Amazon S3-Konsole verwenden, um einen AWS CloudTrail Trail zu konfigurieren, um Datenereignisse für Objekte in einem Amazon S3 on Outposts-Bucket zu protokollieren. CloudTrail unterstützt die Protokollierung von S3 Outposts API Outposts-Operationen auf Objektebene wie `GetObject`, und `DeleteObject`. `PutObject` Diese Ereignisse werden als Datenereignisse bezeichnet.

Standardmäßig protokollieren CloudTrail Trails keine Datenereignisse. Sie können jedoch Trails so konfigurieren, dass Datenereignisse für S3 on Outposts-Buckets, die Sie angeben, oder Datenereignisse für alle S3 on Outposts-Buckets in Ihren protokolliert werden. AWS-Konto


CloudTrail fügt keine Datenereignisse in den Ereignisverlauf ein. CloudTrail Darüber hinaus sind nicht alle API Operationen auf Bucket-Ebene von S3 on Outposts in der Ereignishistorie aufgeführt. CloudTrail Weitere Informationen zum Abfragen von CloudTrail Protokollen finden Sie im AWS Knowledge Center [unter Verwenden von Amazon CloudWatch Logs-Filtermustern und Amazon Athena zum Abfragen von CloudTrail Protokollen](#).

Um einen Trail zum Protokollieren von Datenereignissen für einen S3-in-Outposts-Bucket zu konfigurieren, können Sie entweder die AWS CloudTrail -Konsole oder die Amazon-S3-Konsole verwenden. Wenn Sie einen Trail konfigurieren, um Datenereignisse für alle S3 on Outposts-Buckets in Ihrem zu protokollieren AWS-Konto, ist es einfacher, die CloudTrail Konsole zu verwenden. Informationen zur Verwendung der CloudTrail Konsole zur Konfiguration eines Trails zur Protokollierung von Datenereignissen von S3 on Outposts finden Sie unter [Datenereignisse](#) im AWS CloudTrail Benutzerhandbuch.

Important

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen finden Sie unter [AWS CloudTrail – Preise](#).

Das folgende Verfahren zeigt, wie Sie mit der Amazon S3 S3-Konsole einen CloudTrail Trail zum Protokollieren von Datenereignissen für einen S3 on Outposts-Bucket konfigurieren.

 Note

Derjenige, der den Bucket erstellt AWS-Konto, besitzt ihn und ist der einzige, der S3 on Outposts konfigurieren kann, an die Datenereignisse gesendet werden sollen. AWS CloudTrail

Um die Protokollierung CloudTrail von Datenereignissen für Objekte in einem S3 on Outposts-Bucket zu aktivieren


1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Outposts buckets (Outposts-Buckets) aus.
3. Wählen Sie den Namen des Outposts-Buckets, mit CloudTrail dessen Datenereignissen Sie protokollieren möchten.
4. Wählen Sie Properties (Eigenschaften).
5. Wählen Sie im Bereich AWS CloudTrail Datenereignisse die Option Konfigurieren in CloudTrail aus.

Die AWS CloudTrail Konsole wird geöffnet.

Sie können einen neuen CloudTrail Trail erstellen oder einen vorhandenen Trail wiederverwenden und S3 on Outposts Datenereignisse so konfigurieren, dass sie in Ihrem Trail protokolliert werden.

6. Wählen Sie auf der Dashboard-Seite der CloudTrail Konsole die Option Create Trail aus.
7. Geben Sie auf der Seite Schritt 1 Trail-Attribute auswählen einen Namen für den Trail ein, wählen Sie einen S3-Bucket als Speicherort für die Trail-Protokolle aus, geben Sie alle weiteren gewünschten Einstellungen an und wählen Sie dann Nächstes aus.
8. Wählen Sie auf der Seite Schritt 2 Protokollereignisse auswählen unter Ereignistyp die Option Datenereignisse aus.

Wählen Sie als Datenereignistyp S3 Outposts aus. Wählen Sie Weiter.

 Note

- Wenn Sie einen Trail erstellen und die Datenereignisprotokollierung für S3 in Outposts konfigurieren, müssen Sie den Datenereignistyp korrekt angeben.
- Wenn Sie die CloudTrail Konsole verwenden, wählen Sie S3 Outposts als Daten-Ereignistyp. Informationen zum Erstellen von Trails in der CloudTrail Konsole finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen und Aktualisieren eines Trails mit der Konsole](#). Informationen zur Konfiguration der Datenereignisprotokollierung von S3 on Outposts in der CloudTrail Konsole finden Sie unter [Protokollierung von Datenereignissen für Amazon S3 S3-Objekte](#) im AWS CloudTrail Benutzerhandbuch.
- Wenn Sie das AWS Command Line Interface (AWS CLI) oder das verwenden AWS SDKs, setzen Sie das `resources.type` Feld auf `AWS::S3Outposts::Object`. Weitere Informationen zum Protokollieren von S3 on Outposts-Datenereignissen mit dem AWS CLI finden Sie unter [S3 on Outposts-Ereignisse protokollieren](#) im AWS CloudTrail Benutzerhandbuch.
- Wenn Sie die CloudTrail Konsole oder die Amazon S3 S3-Konsole verwenden, um einen Trail zur Protokollierung von Datenereignissen für einen S3 on Outposts-Bucket zu konfigurieren, zeigt die Amazon S3 S3-Konsole an, dass die Protokollierung auf Objektebene für den Bucket aktiviert ist.

9. Überprüfen Sie auf der Seite Schritt 3 Überprüfen und erstellen die von Ihnen konfigurierten Trail-Attribute und Protokollereignisse. Wählen Sie dann Trail erstellen aus.

So deaktivieren Sie die Protokollierung von CloudTrail Datenereignissen für Objekte in einem S3-Bucket auf Outposts

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im linken Navigationsbereich Trails aus.
3. Wählen Sie den Namen des Trails aus, den Sie erstellt haben, um Ereignisse für den S3-in-Outposts-Bucket zu protokollieren.
4. Wählen Sie oben rechts auf der Detailseite des Trails Protokollierung beenden aus.
5. Wählen Sie im anschließend angezeigten Dialogfeld Protokollierung beenden aus.

Einträge in der AWS CloudTrail Protokolldatei von Amazon S3 on Outposts

Verwaltungsereignisse für Amazon S3 on Outposts sind über AWS CloudTrail verfügbar. Darüber hinaus können Sie optional die [Protokollierung für Datenereignisse aktivieren in AWS CloudTrail](#).

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen S3-Bucket in einer Region übermittelt werden. CloudTrail Logs für Ihre Outposts-Buckets enthalten ein neues Feld, das den Outpost identifiziert `edgeDeviceDetails`, in dem sich der angegebene Bucket befindet.

Zusätzliche Protokollfelder enthalten die angeforderte Aktion, Datum und Uhrzeit der Aktion sowie die Anforderungsparameter. CloudTrail Bei Protokolldateien handelt es sich nicht um einen geordneten Stack-Trace der öffentlichen API Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der eine [PutObject](#)Aktion für `demonstrierts3-outposts`.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:user/yourUserName",
    "accountId": "222222222222",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "yourUserName"
  },
  "eventTime": "2020-11-30T15:44:33Z",
  "eventSource": "s3-outposts.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "26.29.66.20",
  "userAgent": "aws-cli/1.18.39 Python/3.4.10 Darwin/18.7.0 boto3/1.15.39",
  "requestParameters": {
    "expires": "Wed, 21 Oct 2020 07:28:00 GMT",
    "Content-Language": "english",
    "x-amz-server-side-encryption-customer-key-MD5": "wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ObjectCannedACL": "BucketOwnerFullControl",
    "x-amz-server-side-encryption": "Aes256",
    "Content-Encoding": "gzip",
```

```

    "Content-Length": "10",
    "Cache-Control": "no-cache",
    "Content-Type": "text/html; charset=UTF-8",
    "Content-Disposition": "attachment",
    "Content-MD5": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
    "x-amz-storage-class": "Outposts",
    "x-amz-server-side-encryption-customer-algorithm": "Aes256",
    "bucketName": "amzn-s3-demo-bucket1",
    "Key": "path/upload.sh"
  },
  "responseElements": {
    "x-amz-server-side-encryption-customer-key-MD5": "wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "x-amz-server-side-encryption": "Aes256",
    "x-amz-version-id": "001",
    "x-amz-server-side-encryption-customer-algorithm": "Aes256",
    "ETag": "d41d8cd98f00b204e9800998ecf8427f"
  },
  "additionalEventData": {
    "CipherSuite": "ECDHE-RSA-AES128-SHA",
    "bytesTransferredIn": 10,
    "x-amz-id-2": "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"
}
```

Entwickeln mit Amazon S3 on Outposts

Mit Amazon S3 on Outposts können Sie S3-Buckets auf Ihren AWS Outposts erstellen und Objekte für Anwendungen, die lokalen Datenzugriff, lokale Datenverarbeitung und Datenresidenz erfordern, einfach vor Ort speichern und abrufen. S3 on Outposts bietet eine neue Speicherklasse, S3 Outposts (OUTPOSTS), die Amazon S3 verwendet und darauf ausgelegt ist APIs, Daten dauerhaft und redundant auf mehreren Geräten und Servern auf Ihrem zu speichern. AWS Outposts Sie kommunizieren mit Ihrem Outpost-Bucket, indem Sie einen Access Point und eine Endpunktverbindung über eine virtuelle private Cloud (VPC) verwenden. Sie können für Outpost-Buckets dieselben APIs Funktionen wie für Amazon S3 S3-Buckets verwenden, einschließlich Zugriffsrichtlinien, Verschlüsselung und Tagging. Sie können S3 auf Outposts über das AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs, oder REST API verwenden. Weitere Informationen finden Sie unter [Was ist Amazon S3 on Outposts?](#)

Die folgenden Themen enthalten Informationen zur Entwicklung mit S3 on Outposts.

Themen

- [Betrieb von Amazon S3 bei Outposts API](#)
- [Konfigurieren Sie den S3-Kontrollclient für S3 auf Outposts mithilfe von SDK for Java](#)
- [Anfragen an S3 auf Outposts stellen über IPv6](#)

Betrieb von Amazon S3 bei Outposts API

In diesem Thema werden die API Vorgänge Amazon S3, Amazon S3 Control und Amazon S3 on Outposts aufgeführt, die Sie mit Amazon S3 on Outposts verwenden können.

Themen

- [Amazon S3 API S3-Operationen zur Verwaltung von Objekten](#)
- [Amazon S3 API Control-Operationen für die Verwaltung von Buckets](#)
- [S3 on API Outposts-Operationen zur Verwaltung von Outposts](#)

Amazon S3 API S3-Operationen zur Verwaltung von Objekten

S3 on Outposts ist so konzipiert, dass es dieselben API Objektoperationen wie Amazon S3 verwendet. Sie müssen Zugriffspunkte verwenden, um auf ein Objekt in einem Outpost-Bucket

zuzugreifen. Wenn Sie eine API Objektoperation mit S3 auf Outposts verwenden, geben Sie entweder den Outposts-Zugriffspunkt Amazon Resource Name (ARN) oder den Access Point-Alias an. Weitere Informationen zu Zugriffspunkt-Aliassen finden Sie unter [Verwenden eines Alias im Bucket-Stil für den Zugriffspunkt Ihres S3-on-Outposts-Buckets](#).

Amazon S3 on Outposts unterstützt die folgenden Amazon S3 API S3-Operationen:

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [DeleteObjectTagging](#)
- [GetObject](#)
- [GetObjectTagging](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListMultipartUploads](#)
- [ListObjects](#)
- [ListObjectsV2](#)
- [ListObjectVersions](#)
- [ListParts](#)
- [PutObject](#)
- [PutObjectTagging](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Amazon S3 API Control-Operationen für die Verwaltung von Buckets

S3 on Outposts unterstützt die folgenden Amazon S3 API Control-Operationen für die Arbeit mit Buckets.

- [CreateAccessPoint](#)

- [CreateBucket](#)
- [DeleteAccessPoint](#)
- [DeleteAccessPointPolicy](#)
- [DeleteBucket](#)
- [DeleteBucketLifecycleConfiguration](#)
- [DeleteBucketPolicy](#)
- [DeleteBucketReplication](#)
- [DeleteBucketTagging](#)
- [GetAccessPoint](#)
- [GetAccessPointPolicy](#)
- [GetBucket](#)
- [GetBucketLifecycleConfiguration](#)
- [GetBucketPolicy](#)
- [GetBucketReplication](#)
- [GetBucketTagging](#)
- [GetBucketVersioning](#)
- [ListAccessPoints](#)
- [ListRegionalBuckets](#)
- [PutAccessPointPolicy](#)
- [PutBucketLifecycleConfiguration](#)
- [PutBucketPolicy](#)
- [PutBucketReplication](#)
- [PutBucketTagging](#)
- [PutBucketVersioning](#)

S3 on API Outposts-Operationen zur Verwaltung von Outposts

S3 on Outposts unterstützt die folgenden Amazon S3 on API Outposts-Operationen zur Verwaltung von Endpunkten.

- [CreateEndpoint](#)
- [DeleteEndpoint](#)

- [ListEndpoints](#)
- [ListOutpostsWithS3](#)
- [ListSharedEndpoints](#)

Konfigurieren Sie den S3-Kontrollclient für S3 auf Outposts mithilfe von SDK for Java

Im folgenden Beispiel wird der Amazon-S3-Steuerungs-Client für Amazon S3 on Outposts mithilfe von AWS SDK for Java konfiguriert. Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
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();
}
```

Anfragen an S3 auf Outposts stellen über IPv6

Die Dual-Stack-Endpunkte Amazon S3 on Outposts und S3 on Outposts unterstützen Anfragen an S3 on Outposts Buckets, die entweder das Oder-Protokoll verwenden. IPv6 IPv4 Dank der IPv6 Unterstützung für S3 on Outposts können Sie über Netzwerke auf Ihre Buckets zugreifen und diese verwalten und Flugzeugressourcen über S3 on Outposts APIs steuern. IPv6

 Note

[Objektaktionen von S3 on Outposts](#) (wie PutObject oderGetObject) werden in IPv6 Netzwerken nicht unterstützt.

Für den Zugriff auf S3 auf Outposts über IPv6 Netzwerke fallen keine zusätzlichen Gebühren an. Weitere Informationen zu S3 on Outposts finden Sie unter Preise für [S3 on Outposts](#).

Themen

- [Erste Schritte mit IPv6](#)
- [Verwenden von Dual-Stack-Endpunkten, um Anfragen über ein Netzwerk zu stellen IPv6](#)
- [IPv6Adressen in IAM Richtlinien verwenden](#)
- [Testen der IP-Adresskompatibilität](#)
- [Verwenden mit IPv6 AWS PrivateLink](#)
- [Verwendung von S3 auf Dual-Stack-Endpunkten von Outposts](#)

Erste Schritte mit IPv6

Um eine Anfrage an einen S3 on Outposts Bucket über IPv6 zu stellen, müssen Sie einen Dual-Stack-Endpunkt verwenden. Im nächsten Abschnitt wird beschrieben, wie Sie Anfragen mithilfe IPv6 von Dual-Stack-Endpunkten stellen.

Im Folgenden sind wichtige Überlegungen aufgeführt, bevor Sie versuchen, auf einen S3 on Outposts-Bucket zuzugreifen: IPv6

- Der Client und das Netzwerk, die auf den Bucket zugreifen, müssen für die Verwendung IPv6 aktiviert sein.
- Sowohl Anfragen im virtuellen Hosting-Stil als auch im Pfadstil werden für IPv6 den Zugriff unterstützt. Weitere Informationen finden Sie unter [Verwendung von S3 auf Dual-Stack-Endpunkten von Outposts](#).
- Wenn Sie die Quell-IP-Adressfilterung in Ihren AWS Identity and Access Management (IAM) -Benutzer- oder S3 on Outposts-Bucket-Richtlinien verwenden, müssen Sie die Richtlinien aktualisieren, um IPv6 Adressbereiche einzubeziehen.

Note

Diese Anforderung gilt nur für den Bucket-Betrieb von S3 on Outposts und für Ressourcen auf Steuerungsebene in IPv6 Netzwerken. [Objektaktionen von Amazon S3 on Outposts](#) werden IPv6 netzwerkübergreifend nicht unterstützt.

- Bei der Verwendung IPv6 geben Protokolldateien für den Serverzugriff IP-Adressen in einem bestimmten IPv6 Format aus. Sie müssen vorhandene Tools, Skripts und Software aktualisieren, mit denen Sie die Protokolldateien von S3 on Outposts analysieren, damit sie die IPv6 formatierten Remote-IP-Adressen analysieren können. Die aktualisierten Tools, Skripte und Software analysieren dann die formatierten Remote-IP-Adressen korrekt. IPv6

Verwenden von Dual-Stack-Endpunkten, um Anfragen über ein Netzwerk zu stellen IPv6

Um Anfragen mit S3 auf API Outposts-Anrufen zu stellen IPv6, können Sie Dual-Stack-Endpunkte über oder verwenden. AWS CLI AWS SDK Die [API Vorgänge Amazon S3 S3-Steuerung](#) und [S3 on Outposts API](#) funktionieren auf dieselbe Weise, unabhängig davon, ob Sie über ein IPv6 Protokoll oder IPv4 ein Protokoll auf S3 on Outposts zugreifen. Beachten Sie jedoch, dass [S3-Objektaktionen auf Outposts](#) (wie PutObject oder GetObject) nicht über IPv6 Netzwerke unterstützt werden.

Wenn Sie AWS Command Line Interface (AWS CLI) und verwenden AWS SDKs, können Sie einen Parameter oder ein Flag verwenden, um zu einem Dual-Stack-Endpunkt zu wechseln. Sie können den Dual-Stack-Endpunkt auch direkt als Überschreibung des Endpunkts S3 on Outposts in der Konfigurationsdatei angeben.

Sie können einen Dual-Stack-Endpunkt verwenden, um über eine der folgenden Optionen auf einen S3 on IPv6 Outposts-Bucket zuzugreifen:

- Das, siehe AWS CLI. [Verwenden von Dual-Stack-Endpunkten aus dem AWS CLI](#)
- Die AWS SDKs, siehst du [Verwendung von S3 auf Outposts-Dual-Stack-Endpunkten von AWS SDKs](#).

IPv6Adressen in IAM Richtlinien verwenden

Bevor Sie versuchen, mithilfe eines IPv6 Protokolls auf einen S3 on Outposts-Bucket zuzugreifen, stellen Sie sicher, dass die für die IP-Adressfilterung verwendeten IAM Benutzer- oder S3 on Outposts-Bucket-Richtlinien aktualisiert wurden, sodass sie IPv6 Adressbereiche enthalten. Wenn die Richtlinien zur IP-Adressfilterung nicht aktualisiert werden, um IPv6 Adressen zu verarbeiten, können Sie den Zugriff auf einen S3 on Outposts-Bucket verlieren, während Sie versuchen, das IPv6 Protokoll zu verwenden.

IAMRichtlinien, die IP-Adressen filtern, verwenden [Operatoren für IP-Adressbedingungen](#). Die folgende Bucket-Richtlinie für S3 on Outposts identifiziert den IP-Bereich 54.240.143.* zulässiger IPv4 Adressen mithilfe von Operatoren für IP-Adressbedingungen. Allen IP-Adressen außerhalb dieses Bereichs wird der Zugriff auf den S3 on Outposts Bucket (DOC-EXAMPLE-BUCKET) verweigert. Da sich alle IPv6 Adressen außerhalb des zulässigen Bereichs befinden, verhindert diese Richtlinie, dass IPv6 Adressen darauf zugreifen DOC-EXAMPLE-BUCKET können.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3outposts:*",
      "Resource": "arn:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/DOC-EXAMPLE-BUCKET/*",
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"}
      }
    }
  ]
}
```

Sie können das Condition Element der Bucket-Richtlinie S3 on Outposts so ändern, dass sowohl IPv4 (54.240.143.0/24) als auch IPv6 (2001:DB8:1234:5678::/64) Adressbereiche zulässig sind, wie im folgenden Beispiel gezeigt. Sie können denselben Condition Blocktyp wie im Beispiel verwenden, um sowohl Ihre IAM Benutzer- als auch Ihre Bucket-Richtlinien zu aktualisieren.

```
"Condition": {
  "IpAddress": {
```



```
    "aws:SourceIp": [
      "54.240.143.0/24",
      "2001:DB8:1234:5678::/64"
    ]
  }
}
```

Vor der Verwendung müssen IPv6 Sie alle relevanten IAM Benutzer- und Bucket-Richtlinien aktualisieren, die IP-Adressfilterung verwenden, um IPv6 Adressbereiche zuzulassen. Wir empfehlen Ihnen, Ihre IAM Richtlinien zusätzlich zu Ihren bestehenden IPv6 Adressbereichen mit den IPv4 Adressbereichen Ihrer Organisation zu aktualisieren. Ein Beispiel für eine Bucket-Richtlinie, die den Zugriff IPv6 sowohl über als auch ermöglicht IPv4, finden Sie unter [Beschränken des Zugriffs auf bestimmte IP-Adressen](#).

Sie können Ihre IAM Benutzerrichtlinien in der IAM Konsole unter überprüfen <https://console.aws.amazon.com/iam/>. Weitere Informationen zu IAM finden Sie im [IAM Benutzerhandbuch](#). Informationen zur Bearbeitung von Bucket-Richtlinien für S3 on Outposts finden Sie unter [Hinzufügen oder Bearbeiten einer Bucket-Richtlinie für einen Amazon-S3-on-Outposts-Bucket](#).

Testen der IP-Adresskompatibilität

Wenn Sie eine Linux- oder Unix-Instance oder eine MacOS X-Plattform verwenden, können Sie Ihren Zugriff auf einen Dual-Stack-Endpunkt testen. IPv6 Um beispielsweise die Verbindung zu Amazon S3 auf Outposts-Endpunkten zu testen IPv6, verwenden Sie den dig folgenden Befehl:

```
dig s3-outposts.us-west-2.api.aws AAAA +short
```

Wenn Ihr Dual-Stack-Endpunkt über ein IPv6 Netzwerk ordnungsgemäß eingerichtet ist, gibt der dig Befehl die verbundenen Adressen zurück. IPv6 Beispielsweise:

```
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
```

Verwenden mit IPv6 AWS PrivateLink

S3 on Outposts unterstützt das IPv6 Protokoll für AWS PrivateLink Dienste und Endpunkte. Dank der AWS PrivateLink Unterstützung des IPv6 Protokolls können Sie VPC über lokale oder andere private Verbindungen eine Verbindung zu Dienstendpunkten in Ihren IPv6 Netzwerken herstellen. Die IPv6 Unterstützung [AWS PrivateLink für S3 auf Outposts](#) ermöglicht Ihnen auch die Integration AWS PrivateLink mit Dual-Stack-Endpunkten. Eine Anleitung IPv6 zur AWS PrivateLink Aktivierung von finden Sie unter [Beschleunigen Sie Ihre IPv6 Einführung](#) mit Diensten und Endpunkten. AWS PrivateLink

Note

Informationen zum Aktualisieren des unterstützten IP-Adresstyps von IPv4 bis IPv6 finden Sie unter [Ändern des unterstützten IP-Adresstyps](#) im AWS PrivateLink Benutzerhandbuch.

Verwenden IPv6 mit AWS PrivateLink

Wenn Sie AWS PrivateLink with verwendenIPv6, müssen Sie einen IPv6 oder einen VPC Dual-Stack-Schnittstellenendpunkt erstellen. Allgemeine Schritte zum Erstellen eines VPC Endpunkts mit dem AWS Management Console finden Sie unter [Zugreifen auf einen AWS Dienst über einen VPC Schnittstellenendpunkt](#) im AWS PrivateLink Benutzerhandbuch.

AWS Management Console

Gehen Sie wie folgt vor, um einen VPC Schnittstellenendpunkt zu erstellen, der eine Verbindung zu S3 auf Outposts herstellt.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die VPC Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie bei Service category (Servicekategorie) die Option AWS services (-Services) aus.
5. Wählen Sie als Dienstname den Dienst S3 on Outposts (com.amazonaws.us-east-1.s3-outposts).
6. Wählen Sie für die OptionVPC, VPC von der aus Sie auf S3 in Outposts zugreifen möchten.

7. Wählen Sie für Subnetze ein Subnetz pro Availability Zone aus, von dem aus Sie auf S3 on Outposts zugreifen. Sie können nicht mehrere Subnetze aus derselben Availability Zone auswählen. Für jedes Subnetz, das Sie auswählen, wird eine neue Endpunkt-Netzwerkschnittstelle erstellt. Standardmäßig werden IP-Adressen aus den Subnetz-IP-Adressbereichen den Endpunkt-Netzwerkschnittstellen zugewiesen. Um eine IP-Adresse für eine Endpunkt-Netzwerkschnittstelle festzulegen, wählen Sie Designate IP Addresses aus und geben Sie eine IPv6 Adresse aus dem Subnetz-Adressbereich ein.
8. Wählen Sie als IP-Adresstyp Dualstack aus. Weisen Sie Ihren IPv6 Endpunkt-Netzwerkschnittstellen IPv4 sowohl Adressen als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl als auch IPv6 Adressbereiche haben.
9. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Endpunkt-Netzwerkschnittstellen für den VPC Endpunkt zugeordnet werden sollen. Standardmäßig ist die Standardsicherheitsgruppe mit dem verknüpftVPC.
10. Wählen Sie für Richtlinie die Option Vollzugriff aus, um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC Endpunkt zuzulassen. Wählen Sie andernfalls Benutzerdefiniert, um eine VPC Endpunktrichtlinie anzuhängen, die die Berechtigungen steuert, die Principals haben, um Aktionen an Ressourcen über den Endpunkt auszuführen. VPC Diese Option ist nur verfügbar, wenn der Dienst Endpunktrichtlinien unterstütztVPC. Weitere Informationen finden Sie unter [Endpunktrichtlinien](#).
11. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
12. Wählen Sie Endpunkt erstellen.

Example — Bucket-Richtlinie für S3 auf Outposts

Damit S3 on Outposts mit Ihren VPC Endpunkten interagieren kann, können Sie anschließend Ihre Richtlinie für S3 on Outposts wie folgt aktualisieren:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3-outposts:*",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

```
]
}
```

AWS CLI

Note

Um das IPv6 Netzwerk auf Ihrem VPC Endpunkt zu aktivieren, müssen Sie den SupportedIpAddressType Filter für S3 auf Outposts IPv6 eingestellt haben.

Im folgenden Beispiel wird der `create-vpc-endpoint` Befehl verwendet, um einen neuen Dual-Stack-Schnittstellen-Endpunkt zu erstellen.

```
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"
```

Je nach AWS PrivateLink Dienstkonfiguration müssen neu erstellte Endpunktverbindungen möglicherweise vom VPC Endpunktdienstanbieter akzeptiert werden, bevor sie verwendet werden können. Weitere Informationen finden Sie im Benutzerhandbuch unter [Akzeptieren und Ablehnen von Verbindungsanfragen für Endgeräte](#).AWS PrivateLink

Im folgenden Beispiel wird der `modify-vpc-endpoint` Befehl verwendet, um den Endpunkt IPv-only auf einen VPC Dual-Stack-Endpunkt zu aktualisieren. Der Dual-Stack-Endpunkt ermöglicht den Zugriff sowohl auf die als auch auf die Netzwerk IPv4. 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"
```

Weitere Informationen zur Aktivierung des IPv6 Netzwerks für AWS PrivateLink finden Sie unter [Beschleunigen Sie Ihre IPv6 Einführung mit AWS PrivateLink Diensten](#) und Endpunkten.

Verwendung von S3 auf Dual-Stack-Endpunkten von Outposts

S3 auf Outposts Dual-Stack-Endpunkte unterstützen Anfragen an S3 auf Outposts-Buckets über und. IPv6 IPv4 In diesem Abschnitt wird beschrieben, wie Sie S3 auf Dual-Stack-Endpunkten von Outposts verwenden.

Themen

- [S3 auf Outposts Dual-Stack-Endpunkten](#)
- [Verwenden von Dual-Stack-Endpunkten aus dem AWS CLI](#)
- [Verwendung von S3 auf Outposts-Dual-Stack-Endpunkten von AWS SDKs](#)

S3 auf Outposts Dual-Stack-Endpunkten

Wenn Sie eine Anfrage an einen Dual-Stack-Endpunkt stellen, wird der S3 on Outposts-Bucket in eine Adresse IPv6 oder eine Adresse URL aufgelöst. IPv4 Weitere Informationen zum Zugriff auf einen S3 on Outposts Bucket over finden Sie IPv6 unter [Anfragen an S3 auf Outposts stellen über IPv6](#).

Um über einen Dual-Stack-Endpunkt auf einen S3 on Outposts-Bucket zuzugreifen, verwenden Sie einen Endpunktnamen im Pfadstil. S3 on Outposts unterstützt nur regionale Dual-Stack-Endpunktnamen, was bedeutet, dass Sie die Region als Teil des Namens angeben müssen.

Verwenden Sie für einen FIPs Endpunkt im Stil eines Dual-Stack-Pfads die folgende Namenskonvention:

```
s3-outposts-fips.region.api.aws
```

Verwenden Sie für Dual-Stack-Endgeräte, die kein FIPS Endpunkt sind, die folgende Benennungskonvention:

```
s3-outposts.region.api.aws
```

Note

Endpunktnamen im virtuellen Hosted-Stil werden in S3 on Outposts nicht unterstützt.

Verwenden von Dual-Stack-Endpunkten aus dem AWS CLI

Dieser Abschnitt enthält Beispiele für AWS CLI Befehle, mit denen Anfragen an einen Dual-Stack-Endpunkt gestellt werden. Anweisungen zur Einrichtung von finden Sie AWS CLI unter [Erste Schritte mit der Verwendung von AWS CLI und SDK für Java](#).

Sie legen den Konfigurationswert `true` in einem Profil in Ihrer AWS Config Datei `use_dualstack_endpoint` auf fest, um alle Amazon S3 S3-Anfragen, die von den `s3api` AWS CLI Befehlen `s3` und gestellt werden, an den Dual-Stack-Endpunkt für die angegebene Region weiterzuleiten. Sie geben die Region in der Konfigurationsdatei oder in einem Befehl mit der `--region` Option an.

Bei der Verwendung von Dual-Stack-Endpunkten mit dem AWS CLI wird nur der `path` Adressierungsstil unterstützt. Der in der Konfigurationsdatei festgelegte Adressierungsstil bestimmt, ob der Bucket-Name im Hostnamen oder im. URL Weitere Informationen finden Sie unter [s3outposts](#) im AWS CLI -Benutzerhandbuch.

Um einen Dual-Stack-Endpunkt über den zu verwenden AWS CLI, verwenden Sie den `--endpoint-url` Parameter mit dem `https://s3-outposts-fips.region.api.aws` Endpunkt `http://s3.dualstack.region.amazonaws.com` oder für beliebige OR-Befehles `s3control.s3outposts`

Beispielsweise:

```
$ aws s3control list-regional-buckets --endpoint-url https://s3-outposts.region.api.aws
```

Verwendung von S3 auf Outposts-Dual-Stack-Endpunkten von AWS SDKs

Dieser Abschnitt enthält Beispiele für den Zugriff auf einen Dual-Stack-Endpunkt mithilfe von. AWS SDKs

AWS SDK for Java 2.x Beispiel für einen -Dual-Stack-Endpunkt

Die folgenden Beispiele zeigen, wie Sie die `S3OutpostsClient` Klassen `S3ControlClient` und verwenden, um Dual-Stack-Endpunkte zu aktivieren, wenn Sie einen S3-on-Outposts-Client mit dem erstellen. AWS SDK for Java 2.x Anweisungen zum Erstellen und Testen eines funktionierenden Java-Beispiels für Amazon S3 auf Outposts finden Sie unter [Erste Schritte mit der Verwendung von AWS CLI und SDK für Java](#).

Example — Erstellen Sie eine `S3ControlClient` Klasse mit aktivierten Dual-Stack-Endpunkten

```
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 — Erstellen Sie eine **S3OutpostsClient** mit aktivierten Dual-Stack-Endpunkten

```

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();
    }
}
}
```

Wenn Sie das AWS SDK for Java 2.x unter Windows verwenden, müssen Sie möglicherweise die folgende Java-Eigenschaft für virtuelle Maschinen (JVM) festlegen:

```
java.net.preferIPv6Addresses=true
```

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.