



User Guide

AWS DataSync



AWS DataSync: User Guide

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. 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 AWS DataSync?	1
Anwendungsfälle	2
Vorteile	2
Weitere Ressourcen	3
Funktionsweise	4
DataSync Architektur der Übertragung	4
Übertragung zwischen lokalem Speicher und AWS	4
Übertragung zwischen AWS Speicherdiensten	5
Übertragung zwischen AWS Speicherdiensten und Speichersystemen in anderen Clouds	6
Konzepte und Terminologie	7
Agent	8
Speicherort	8
Aufgabe	8
Ausführung der Aufgabe	8
Wie werden Dateien, Objekte und Verzeichnisse DataSync übertragen	9
Wie wird Ihre Datenübertragung DataSync vorbereitet	9
Wie werden deine DataSync Daten übertragen	10
Wie DataSync wird die Integrität Ihrer Daten überprüft	11
Wie DataSync funktioniert mit geöffneten und gesperrten Dateien	12
Optionen für wiederkehrende Übertragungen	12
Erste Schritte	13
Melde dich an für ein AWS-Konto	13
Erstellen eines Benutzers mit Administratorzugriff	13
Erforderliche IAM-Berechtigungen für die Verwendung DataSync	15
AWS verwaltete Richtlinien	15
Kundenverwaltete Richtlinien	15
Wo kann ich verwenden? DataSync	16
Wie kann ich verwenden? DataSync	16
Wie viel wird es DataSync kosten?	16
Open-Source-Komponenten, die verwendet werden von DataSync	16
Brauche ich einen Agenten?	16
Situationen, in denen Sie einen DataSync Agenten benötigen	17
Situationen, in denen Sie keinen DataSync Agenten benötigen	17
Wählen Sie einen Agenten für Ihren Aufgabenmodus	17

Verwendung mehrerer DataSync Agenten	18
Nächste Schritte	19
Anforderungen an Agenten	19
Hypervisor-Anforderungen	19
Anforderungen an den Agenten für DataSync Übertragungen	20
Agentenanforderungen für Partitionen AWS-Region	22
Anforderungen an die Agentenverwaltung	22
Setzen Sie Ihren Agenten ein	22
Bereitstellen Sie Ihren Agenten auf VMware	23
Bereitstellen Ihres Agenten auf KVM	23
Bereitstellen Ihres Agenten im Basismodus auf Microsoft Hyper-V	25
Bereitstellung Ihres EC2 Amazon-Agenten	26
Bereitstellen Ihres Agenten im Basismodus auf AWS Outposts	31
Wählen Sie einen Service-Endpunkt für Ihren Agenten	31
Auswahl eines Endpunkts für öffentliche Dienste	32
Auswahl eines FIPS-Serviceendpunkts	32
Auswahl eines VPC-Serviceendpunkts	33
Ihren Agenten aktivieren	35
Voraussetzungen	35
Einen Aktivierungsschlüssel erhalten	36
Ihren Agenten aktivieren	38
Nächste Schritte	42
Überprüfen Sie die Netzwerkverbindungen Ihres Agenten	42
Greifen Sie auf die lokale Konsole Ihres Agenten zu	42
Überprüfen Sie die Verbindung Ihres Agenten zu Ihrem Speichersystem	43
Überprüfen Sie die Verbindung Ihres Agenten mit dem Dienst DataSync	44
Nächste Schritte	45
Ihr Netzwerk verbinden	46
1. Netzwerkverbindung zwischen Ihrem Speichersystem und dem Agenten	46
2. Netzwerkverbindung zwischen Ihrem Agenten und DataSync dem Service	46
Verbinden Sie Ihr Speichernetzwerk mit AWS	47
Auswählen eines Service-Endpunkts	47
3. Netzwerkverbindung zwischen DataSync Dienst und AWS Speicherdienst	48
Netzwerkbetrieb, wenn Sie keinen DataSync Agenten benötigen	48
Wie und wo der DataSync Verkehr durch das Netzwerk fließt	48
Netzwerksicherheit für DataSync	48

Netzwerkanforderungen	49
IPv6 Unterstützung	49
Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher	50
Netzwerkanforderungen für AWS Speicherdienste	55
Netzwerkanforderungen für öffentliche Endpunkte oder FIPS-Dienstendpunkte	56
Netzwerkanforderungen für VPC- oder FIPS-VPC-Dienstendpunkte	64
Netzwerkschnittstellen für Datenübertragungen	68
Netzwerkschnittstellen für Übertragungen mit Agenten	68
Netzwerkschnittstellen für Übertragungen ohne Agenten	69
Ihre Netzwerkschnittstellen anzeigen	70
Architektur- und Routing-Beispiele mit Direct Connect	71
Verwenden von Direct Connect mit einem DataSync VPC-Serviceendpunkt	71
Verwenden von Direct Connect mit einem DataSync öffentlichen oder FIPS- Serviceendpunkt	75
Nächste Schritte	75
Konfiguration Ihres Agenten für mehrere NICs	76
Datenübertragung	77
Wo kann ich meine Daten übertragen?	78
Unterstützte Übertragungen im selben AWS-Konto	78
Unterstützte Übertragungen zwischen AWS-Konten	80
Unterstützte Übertragungen im selben AWS-Region	81
Unterstützte Übertragungen zwischen AWS-Regionen	81
Stellen Sie fest, ob für Ihre Übertragung ein Agent erforderlich ist DataSync	82
Übertragung in oder aus einem lokalen Speicher	82
Konfiguration von Übertragungen mit einem NFS-Dateiserver	82
Konfiguration von Übertragungen mit einem SMB-Dateiserver	87
Konfiguration von Übertragungen mit einem HDFS-Cluster	98
Konfiguration von Übertragungen mit einem Objektspeichersystem	103
Übertragung in den oder aus dem AWS Speicher	108
Konfiguration von Übertragungen mit Amazon S3	108
Konfiguration von Übertragungen mit Amazon EFS	143
Konfiguration von Übertragungen mit FSx für Windows File Server	153
Transfers mit FSx for Lustre konfigurieren	158
Konfiguration von Übertragungen mit FSx für OpenZFS	160
Konfiguration von Übertragungen mit FSx für ONTAP	164
Übertragung zu oder von einem anderen Cloud-Speicher	172

Planung von Übertragungen zu oder von Cloud-Speichersystemen von Drittanbietern	173
Übertragungen mit Google Cloud Storage konfigurieren	175
Übertragungen konfigurieren mit Microsoft Azure Blob Storage	186
Transfers konfigurieren mit Microsoft Azure Files	204
Konfiguration von Übertragungen mit anderem Cloud-Objektspeicher	208
Eine Aufgabe für die Übertragung von Daten erstellen	215
Ihre Aufgabe erstellen	215
Status der Aufgaben	218
Partitionierung großer Datensätze mit mehreren Aufgaben	219
Segmentierung übertragener Daten mit mehreren Aufgaben	219
Wählen Sie einen Aufgabenmodus für Ihre Übertragung	220
Auswahl der zu übertragenden Daten	225
Überprüfung der Datenintegrität	266
Festlegung von Bandbreitenbeschränkungen	269
Planung Ihrer Aufgabe	271
Verschlagworten Sie Ihre Aufgaben	276
Eine Aufgabe zur Übertragung von Daten starten	280
Starten Sie Ihre Aufgabe	280
Status der Aufgabenausführung	281
Wissen Sie, wann sich Ihre Aufgabe in der Warteschlange befindet	283
Die Ausführung Ihrer Aufgabe wird abgebrochen	283
Überwachung von Datenübertragungen	285
Leistungsindikatoren für die Datenübertragung verstehen	285
Überwachung von Datenübertragungen mit CloudWatch Metriken	311
CloudWatch Metriken für DataSync	311
Überwachung von Datenübertragungen mit Aufgabenberichten	316
Anwendungsfälle	316
Aufgabenberichte nur zusammenfassend	317
Standardberichte für Aufgaben	317
Beispiele für Aufgabenberichte	320
Einschränkungen	324
Erstellen Sie Ihre Aufgabenberichte	324
Ihre Aufgabenberichte anzeigen	335
Überwachung von Datenübertragungen mit CloudWatch Logs	336
Ermöglicht DataSync das Hochladen von Protokollen in eine CloudWatch Protokollgruppe .	336
Konfiguration der Protokollierung für Ihre DataSync Aufgabe	338

DataSync Task-Protokolle anzeigen	342
Protokollierung mit CloudTrail	343
Arbeiten mit DataSync Informationen in CloudTrail	343
DataSync Logdateieinträge verstehen	344
Überwachung mit EventBridge	346
DataSync Ereignisse übertragen	346
Überwachung mit manuellen Tools	348
Überwachen Sie Ihre Übertragung mithilfe der DataSync Konsole	349
Überwachen Sie Ihre Übertragung mithilfe der AWS CLI	349
Überwachen Sie Ihre Übertragung mithilfe des watch Dienstprogramms	351
Verwalten von Ressourcen	352
Ihren DataSync Agenten verwalten	352
Testen der Konnektivität und der Systemressourcen Ihres DataSync Agenten	352
Ihren DataSync Agenten ersetzen	352
DataSync Ressourcen bereinigen	352
Die Infrastruktur eines DataSync Agenten wiederverwenden	352
Verwaltung Ihres Agenten	353
Softwareupdates für Agenten	353
Status der Agenten	353
Problembehebung bei Ihrem Agenten	354
Durchführung von Wartungsarbeiten an Ihrem Agenten	354
Greifen Sie auf die lokale Konsole Ihres Agenten zu	355
Konfiguration der DHCP-, DNS- und IP-Einstellungen Ihres Agenten	356
Überprüfen Sie die Systemressourcen Ihres Agenten	361
Serverkonfiguration für die Systemzeit des Agenten anzeigen und verwalten	362
Befehle im Zusammenhang mit der Wartung für Ihren Agenten ausführen	364
Ihren Agenten ersetzen	365
Einen neuen Agenten erstellen	366
Aktualisierung Ihres Standorts mit dem neuen Agenten	366
Nächste Schritte	372
DataSync Ressourcen filtern	373
Parameter für die Filterung	373
Nach Standort filtern	374
Nach Aufgabe filtern	375
DataSync Ressourcen aufräumen	376
Einen DataSync Agenten löschen	376

Die Infrastruktur eines DataSync Agenten wiederverwenden	377
Löschen eines DataSync Standorts	378
Eine DataSync Aufgabe löschen	378
Sicherheit	380
Datenschutz	381
Verschlüsselung während der Übertragung	381
Verschlüsselung im Ruhezustand	384
Richtlinie für den Datenverkehr zwischen Netzwerken	385
Identity and Access Management	385
Zugriffsverwaltung	386
AWS verwaltete Richtlinien	392
Kundenverwaltete Richtlinien	400
Verwenden von servicegebundenen Rollen	403
Markieren von Ressourcen während der Erstellung	408
Serviceübergreifende Confused-Deputy-Prävention	410
Compliance-Validierung	411
Ausfallsicherheit	412
Sicherheit der Infrastruktur	412
Sicherung der Anmeldeinformationen für den Speicherort	413
Verwenden eines vom Service verwalteten Geheimnisses, das mit einem Standardschlüssel verschlüsselt ist	414
Es wird ein vom Service verwaltetes Geheimnis verwendet, das mit einem benutzerdefinierten AWS KMS Schlüssel verschlüsselt ist	414
Verwenden Sie ein Geheimnis, das Sie verwalten	416
Kontingente	420
Speichersystem-, Datei- und Objektbeschränkungen	420
DataSync Kontingente	420
Anfordern einer Kontingenterhöhung	426
Fehlerbehebung	427
Behebung von Problemen mit Agenten	427
Wie stelle ich eine Verbindung zur lokalen Konsole eines EC2 Amazon-Agenten her?	427
Was bedeutet der Fehler Fehler beim Abrufen des Agenten-Aktivierungsschlüssels?	428
Ich kann einen Agenten immer noch nicht mithilfe eines VPC-Dienstendpunkts aktivieren ...	428
Was mache ich, wenn mein Agent offline ist?	428
Ich weiß nicht, was mit meinem Agenten los ist. Kann mir jemand helfen?	429
Behebung von Standortproblemen	430

Meine Aufgabe ist mit der Fehlermeldung „NFS-Berechtigungen verweigert“ fehlgeschlagen	431
Meine Aufgabe ist mit einem NFS-Mount-Fehler fehlgeschlagen	431
Meine Aufgabe ist mit einem Amazon EFS-Mount-Fehler fehlgeschlagen	432
Der Dateibesitz wird bei der NFS-Übertragung nicht beibehalten	432
Meine Aufgabe kann nicht auf einen SMB-Standort zugreifen, der Kerberos verwendet	433
Meine Aufgabe ist mit einem input/output Fehler fehlgeschlagen	434
Fehler: FsS3UnableToConnectToEndpoint	435
Fehler: FsS3HeadBucketFailed	435
Die Aufgabe schlägt mit einem Unable to list Azure Blobs on the volume root Fehler fehl	436
Fehler: FsAzureBlobVolRootListBlobsFailed	436
Fehler: SrcLocHitAccess	436
Fehler: SyncTaskErrorLocationNotAdded	437
Fehler: S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation	437
Die Aufgabe mit dem S3-Quellspeicherort schlägt mit HeadObject oder mit einem GetObjectTagging Fehler fehl	437
Behebung von Problemen mit Aufgaben	438
Fehler: Ungültiger SyncOption Wert. Option: TransferModePreserveDeletedFiles, Wert: ALL, REMOVE.	438
Die Ausführung der Aufgabe schlägt mit einem EniNotFoundFehler fehl	438
Die Ausführung der Aufgabe schlägt fehl und es wird der Fehler „Speicher kann nicht zugewiesen werden“ angezeigt	439
Die Aufgabe schlägt mit oder Input/Output error FSx für das ONTAP-Dateisystem fehl	439
Die Aufgabe schlägt fehl mit Connection Reset by peer oder Host is down Meldung FSx für das ONTAP-Dateisystem	441
Die Ausführung der Aufgabe hat einen Startstatus, aber es scheint nichts zu passieren	442
Die Aufgabenausführung scheint im Vorbereitungsstatus stecken geblieben zu sein	443
Die Ausführung der Aufgabe wird beendet, bevor die Übertragung abgeschlossen ist	443
Die Ausführung der Aufgabe schlägt fehl, wenn sie aus einem Google Cloud Storage-Bucket übertragen wird	443
Es gibt Diskrepanzen zwischen den Zeitstempeln der Aufgabenausführung	444
Die Ausführung der Aufgabe schlägt mit einem NoMem Fehler fehl	444
Die Ausführung der Aufgabe schlägt mit einem FsNfsIdMappingEnabled Fehler fehl	444

Das Objekt kann nicht übertragen werden (Fehler) Azure Blob Storage user metadata key	445
Am Zielort / .aws-datasync befindet sich ein Ordner	445
Symbolische Links können mit SMB nicht zwischen Standorten übertragen werden	445
Aufgabe: Fehler melden	446
Behebung von Problemen bei der Datenüberprüfung	446
Es gibt Diskrepanzen zwischen den Inhalten einer Datei	447
Die SMB-Metadaten einer Datei stimmen nicht überein	448
Die zu übertragenden Dateien befinden sich nicht mehr am Quellspeicherort	449
DataSync kann die Zieldaten nicht verifizieren	450
DataSync kann Objektmustern nicht lesen	451
Die systemdefinierten Metadaten eines Objekts stimmen nicht überein	451
Grundlegendes zur Dauer der Datenüberprüfung	453
Fehlerbehebung bei S3-Speicherkosten mit DataSync	453
Lernprogramme	455
Kontoübergreifende Übertragung vom lokalen Standort auf S3	455
-Übersicht	455
Voraussetzung: Erforderliche Quellkontoberechtigungen	456
Voraussetzung: Erforderliche Berechtigungen für das Zielkonto	459
Schritt 1: Erstellen Sie in Ihrem Quellkonto einen DataSync Agenten	459
Schritt 2: Erstellen Sie in Ihrem Quellkonto eine DataSync IAM-Rolle für den Zugriff auf den Ziel-Bucket	460
Schritt 3: Aktualisieren Sie in Ihrem Zielkonto Ihre S3-Bucket-Richtlinie	462
Schritt 4: Deaktivieren Sie in Ihrem Zielkonto die Option ACLs für Ihren S3-Bucket	464
Schritt 5: Erstellen Sie in Ihrem Quellkonto einen DataSync Quellspeicherort für Ihren lokalen Speicher	464
Schritt 6: Erstellen Sie in Ihrem Quellkonto einen DataSync Zielort für Ihren S3-Bucket	464
Schritt 7: Erstellen und starten Sie in Ihrem Quellkonto Ihre DataSync Aufgabe	466
Zugehörige Ressourcen	466
Übertragung zwischen S3-Buckets zwischen Konten	468
-Übersicht	468
Voraussetzung: Erforderliche Quellkontoberechtigungen	470
Voraussetzung: Erforderliche Berechtigungen für das Zielkonto	473
Schritt 1: Erstellen Sie in Ihrem Quellkonto eine DataSync IAM-Rolle für den Zugriff auf den Ziel-Bucket	473
Schritt 2: Aktualisieren Sie in Ihrem Zielkonto Ihre S3-Bucket-Richtlinie	475

Schritt 3: Deaktivieren Sie in Ihrem Zielkonto die Option ACLs für Ihren S3-Bucket	477
Schritt 4: Erstellen Sie in Ihrem Quellkonto Ihre DataSync Standorte	477
Schritt 5: Erstellen und starten Sie in Ihrem Quellkonto Ihre DataSync Aufgabe	480
Fehlerbehebung	481
Verwandt: Kontoübergreifende Übertragungen mit S3-Buckets unter Verwendung serverseitiger Verschlüsselung	480
Durchführung einer großen Migration	483
Was ist eine umfangreiche Datenmigration?	483
Die wichtigsten Phasen einer Migration großer Datenmengen	483
Weitere Ressourcen	484
Phase 1: Planung Ihrer Migration	484
Erfassung der Anforderungen	485
Ausführen eines Machbarkeitsnachweises	491
Schätzung der Migrationszeitpläne	493
Phase 2: Implementierung Ihrer Migration	495
Beschleunigen Sie Ihre Migration durch Partitionierung	496
Ihre DataSync Aufgaben ausführen	497
Überwachen Sie Ihre Übertragungen	499
DataSync API	500
Aktionen	500
CancelTaskExecution	503
CreateAgent	505
CreateLocationAzureBlob	510
CreateLocationEfs	517
CreateLocationFsxLustre	524
CreateLocationFsxOntap	528
CreateLocationFsxOpenZfs	533
CreateLocationFsxWindows	538
CreateLocationHdfs	543
CreateLocationNfs	551
CreateLocationObjectStorage	556
CreateLocationS3	564
CreateLocationSmb	569
CreateTask	579
DeleteAgent	589
DeleteLocation	591

DeleteTask	593
DescribeAgent	595
DescribeLocationAzureBlob	600
DescribeLocationEfs	605
DescribeLocationFsxLustre	611
DescribeLocationFsxOntap	614
DescribeLocationFsxOpenZfs	619
DescribeLocationFsxWindows	623
DescribeLocationHdfs	627
DescribeLocationNfs	632
DescribeLocationObjectStorage	636
DescribeLocationS3	641
DescribeLocationSmb	646
DescribeTask	653
DescribeTaskExecution	663
ListAgents	685
ListLocations	689
ListTagsForResource	693
ListTaskExecutions	697
ListTasks	701
StartTaskExecution	705
TagResource	712
UntagResource	715
UpdateAgent	718
UpdateLocationAzureBlob	720
UpdateLocationEfs	725
UpdateLocationFsxLustre	729
UpdateLocationFsxOntap	732
UpdateLocationFsxOpenZfs	735
UpdateLocationFsxWindows	738
UpdateLocationHdfs	742
UpdateLocationNfs	748
UpdateLocationObjectStorage	751
UpdateLocationS3	757
UpdateLocationSmb	761
UpdateTask	769

UpdateTaskExecution	776
Datentypen	778
AgentListEntry	781
AzureBlobSasConfiguration	783
CmkSecretConfig	784
CustomSecretConfig	786
Ec2Config	788
FilterRule	790
FsxProtocol	792
FsxProtocolNfs	793
FsxProtocolSmb	794
FsxUpdateProtocol	796
FsxUpdateProtocolSmb	798
HdfsNameNode	800
LocationFilter	802
LocationListEntry	804
ManagedSecretConfig	806
ManifestConfig	807
NfsMountOptions	809
OnPremConfig	811
Options	812
Platform	821
PrivateLinkConfig	822
QopConfiguration	824
ReportDestination	825
ReportDestinationS3	826
ReportOverride	828
ReportOverrides	829
ReportResult	831
S3Config	833
S3ManifestConfig	834
SmbMountOptions	836
SourceManifestConfig	838
TagListEntry	839
TaskExecutionFilesFailedDetail	840
TaskExecutionFilesListedDetail	842

TaskExecutionFoldersFailedDetail	844
TaskExecutionFoldersListedDetail	846
TaskExecutionListEntry	848
TaskExecutionResultDetail	850
TaskFilter	853
TaskListEntry	855
TaskReportConfig	857
TaskSchedule	859
TaskScheduleDetails	861
Häufige Fehler	862
Geläufige Parameter	864
Dokumentverlauf	867
AWS Glossar	883
.....	dccclxxxiv

Was ist AWS DataSync?

AWS DataSync ist ein sicherer, zuverlässiger und schneller Dateiübertragungsdienst, mit dem Sie Ihre Datei- oder Objektdaten schnell und einfach zu, von und zwischen AWS Speicherdiensten übertragen können.

Speicherübertragungen vor Ort

DataSync funktioniert mit den folgenden lokalen Speichersystemen:

- [Network File System \(NFS\)](#)
- [Server Message Block \(SMB\)](#)
- [Verteilte Hadoop-Dateisysteme \(HDFS\)](#)
- [Objektspeicher](#)

AWS Speicherübertragungen

DataSync funktioniert mit den folgenden AWS Speicherdiensten:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Amazon FSx für Windows-Dateiserver](#)
- [Amazon FSx für Lustre](#)
- [Amazon FSx für OpenZFS](#)
- [Amazon FSx für NetApp ONTAP](#)

Andere Cloud-Speicherübertragungen

DataSync funktioniert mit den folgenden Speicherdiensten in anderen Clouds:

- [Google Cloud Storage](#)
- [Microsoft Azure Blob Storage](#)
- [Microsoft Azure Files](#)
- [Wasabi Cloud Storage](#)
- [DigitalOcean Spaces](#)

- [Oracle Cloud Infrastructure Object Storage](#)
- [Cloudflare R2 Storage](#)
- [Backblaze B2 Cloud Storage](#)
- [NAVER Cloud Object Storage](#)
- [Alibaba Cloud Object Storage Service](#)
- [IBM Cloud Object Storage](#)
- [Seagate Lyve Cloud](#)

Anwendungsfälle

Dies sind einige der wichtigsten Anwendungsfälle für DataSync:

- **Daten migrieren** — Schnelle Übertragung aktiver Datensätze über das Netzwerk in AWS Speicherdienste. DataSync beinhaltet automatische Verschlüsselung und Überprüfung der Datenintegrität, um sicherzustellen, dass Ihre Daten sicher, unversehrt und einsatzbereit ankommen.
- **Archivierung kalter Daten** — Verschieben Sie kalte Daten, die im lokalen Speicher gespeichert sind, direkt in langlebige und sichere Langzeitspeicherklassen wie S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive. Auf diese Weise können Sie lokale Speicherkapazität freisetzen und ältere Systeme herunterfahren.
- **Daten replizieren** — Kopieren Sie Daten in die meisten Amazon S3 S3-Speicherklassen und wählen Sie die kostengünstigste Lösung für Ihre Bedürfnisse. Sie können auch Daten an Amazon EFS oder Amazon FSx für ein Standby-Dateisystem senden.
- **Daten für eine zeitnahe Verarbeitung in der Cloud übertragen** — Daten zur Verarbeitung in oder aus der AWS Cloud übertragen. Dieser Ansatz kann in zahlreichen Branchen kritische Hybrid-Cloud-Workflows beschleunigen. Dazu gehören maschinelles Lernen in der Biowissenschaftsbranche, Videoproduktion in Medien und Unterhaltung, Big-Data-Analysen bei Finanzdienstleistungen und seismische Forschung in der Öl- und Gasindustrie.

Vorteile

Durch die Verwendung können Sie DataSync die folgenden Vorteile erzielen:

- **Automatisieren Sie die Datenbewegung** — DataSync erleichtert die Übertragung von Daten über das Netzwerk zwischen Speichersystemen und Diensten. DataSync automatisiert sowohl das

Management von Datenübertragungsprozessen als auch die Infrastruktur, die für leistungsstarke und sichere Datenübertragungen erforderlich ist.

- **Sichere Datenübertragung** — DataSync bietet end-to-end Sicherheit, einschließlich Verschlüsselung und Überprüfung der Datenintegrität, um sicherzustellen, dass Ihre Daten sicher, unversehrt und einsatzbereit ankommen. DataSync greift über integrierte AWS Sicherheitsmechanismen wie AWS Identity and Access Management (IAM-) Rollen auf Ihren AWS Speicher zu. Es unterstützt auch Virtual Private Cloud (VPC) -Endpunkte, sodass Sie Daten übertragen können, ohne das öffentliche Internet zu durchqueren, und die Sicherheit von online kopierten Daten weiter erhöht.
- **Daten schneller übertragen** — DataSync verwendet ein speziell entwickeltes Netzwerkprotokoll und eine parallel Multithread-Architektur, um Ihre Übertragungen zu beschleunigen. Dieser Ansatz beschleunigt Migrationen, wiederkehrende Datenverarbeitungsworkflows für Analysen und maschinelles Lernen sowie Datenschutzprozesse.

Weitere Ressourcen

Sie sollten Folgendes lesen:

- [DataSync Ressourcen](#) — Beinhaltet Blogs, Videos und anderes Schulungsmaterial
- [AWS re:POST](#) — Sehen Sie sich die neueste Diskussion rund um DataSync
- [AWS DataSync -Preise](#)

Wie AWS DataSync funktioniert

Lernen Sie die wichtigsten Konzepte und Begriffe im Zusammenhang mit AWS DataSync Übertragungen kennen, einschließlich der Art und Weise, wie Daten von lokalen und Cloud-Standorten übertragen werden.

DataSync Architektur der Übertragung

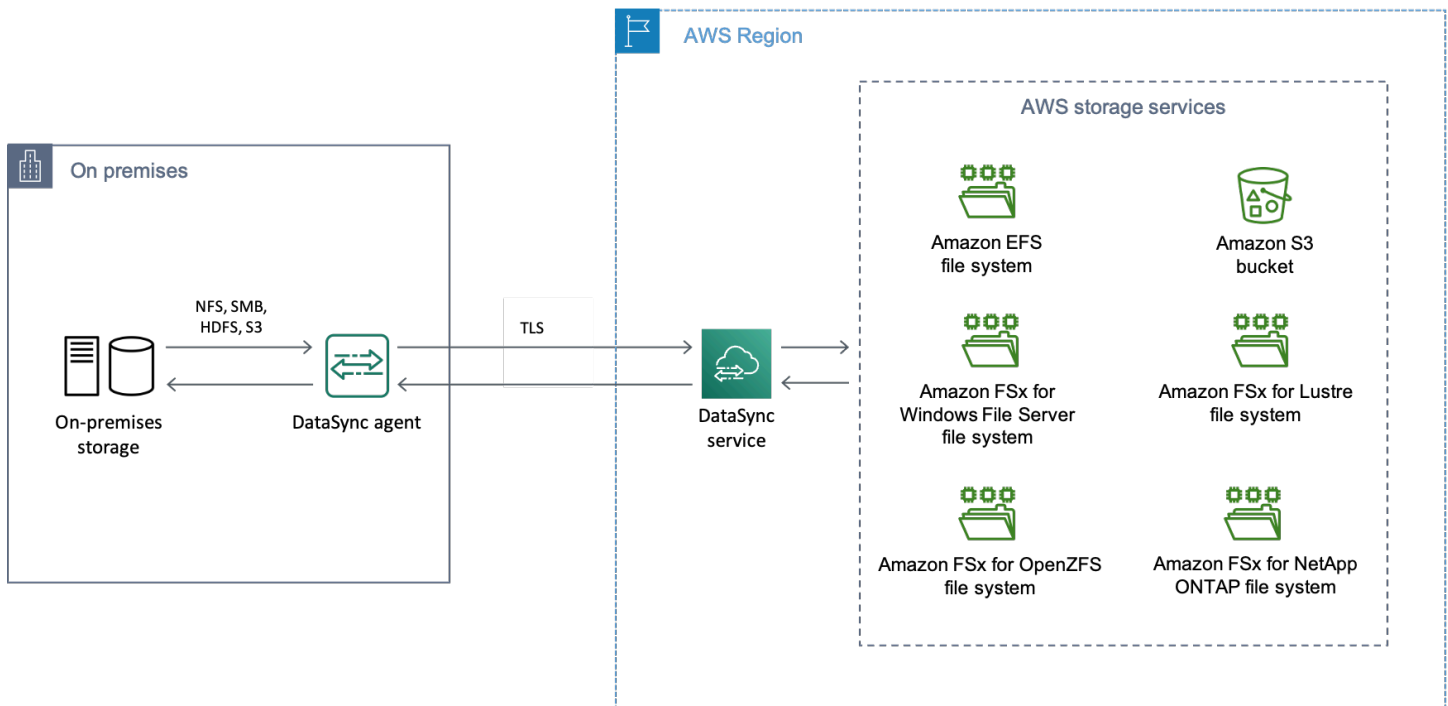
Die folgenden Diagramme zeigen, wie und wo Speicherdaten DataSync üblicherweise übertragen werden. Eine vollständige Liste der DataSync unterstützten Speichersysteme und Dienste finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#)

Themen

- [Übertragung zwischen lokalem Speicher und AWS](#)
- [Übertragung zwischen AWS Speicherdiensten](#)
- [Übertragung zwischen AWS Speicherdiensten und Speichersystemen in anderen Clouds](#)

Übertragung zwischen lokalem Speicher und AWS

Das folgende Diagramm zeigt einen allgemeinen Überblick über die DataSync Übertragung von Dateien zwischen selbstverwalteten, lokalen Speichersystemen und AWS-Services

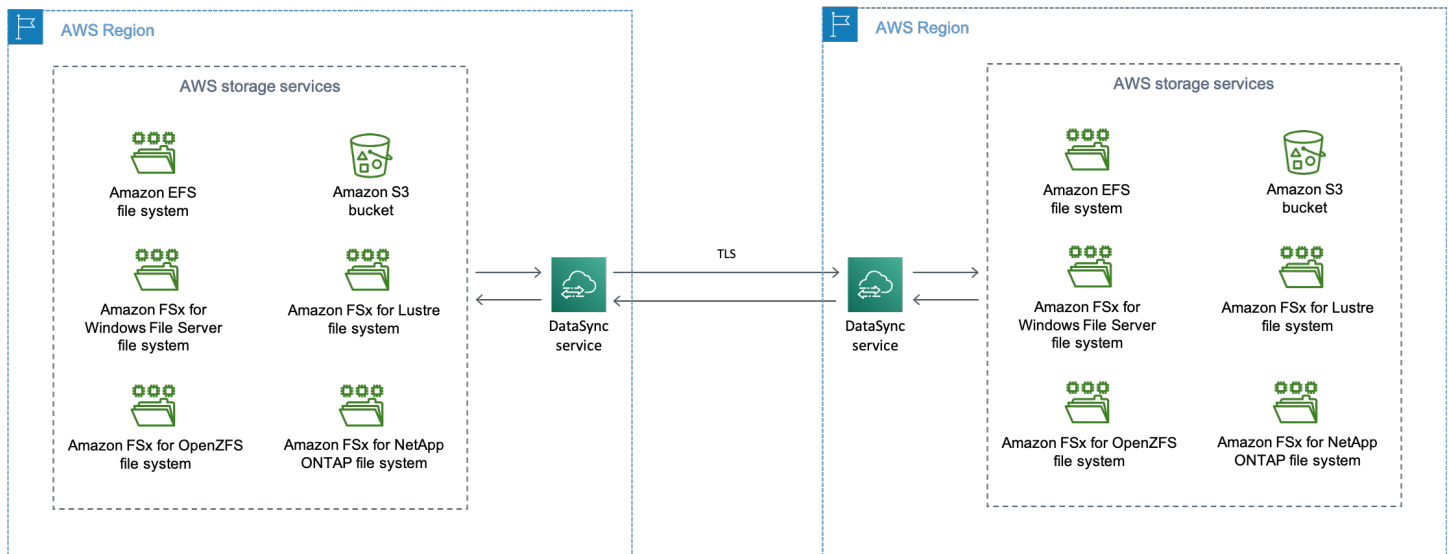


Das Diagramm veranschaulicht einen häufigen DataSync Anwendungsfall:

- Ein DataSync Agent, der Daten aus einem lokalen Speichersystem kopiert.
- Daten werden übertragen AWS und mit Transport Layer Security (TLS) verschlüsselt.
- DataSync Daten in einen unterstützten AWS Speicherdienst kopieren.

Übertragung zwischen AWS Speicherdiensten

Das folgende Diagramm zeigt einen allgemeinen Überblick über die DataSync Übertragung von Dateien zwischen AWS-Services denselben Dateien AWS-Konto.



Das Diagramm veranschaulicht einen häufigen DataSync Anwendungsfall:

- DataSync Kopieren von Daten aus einem unterstützten AWS Speicherdienst.
- Übertragung von Daten AWS-Regionen, verschlüsselt mit TLS.
- DataSync Daten in einen unterstützten AWS Speicherdienst kopieren.

Bei der Übertragung zwischen AWS Speicherdiensten in demselben Konto (unabhängig davon, ob sie sich in derselben Partition AWS-Region oder AWS-Regionen in derselben Partition befinden), ist kein Agent erforderlich. Ihre Daten verbleiben im AWS Netzwerk und werden nicht über das öffentliche Internet übertragen.

Important

Sie zahlen für Daten, die zwischen AWS-Regionen diesen übertragen werden. Dies wird als AUSGEHENDE Datenübertragung von Ihrer Quellregion in Ihre Zielregion abgerechnet. Weitere Informationen finden Sie unter [Preise für Datenübertragungen](#).

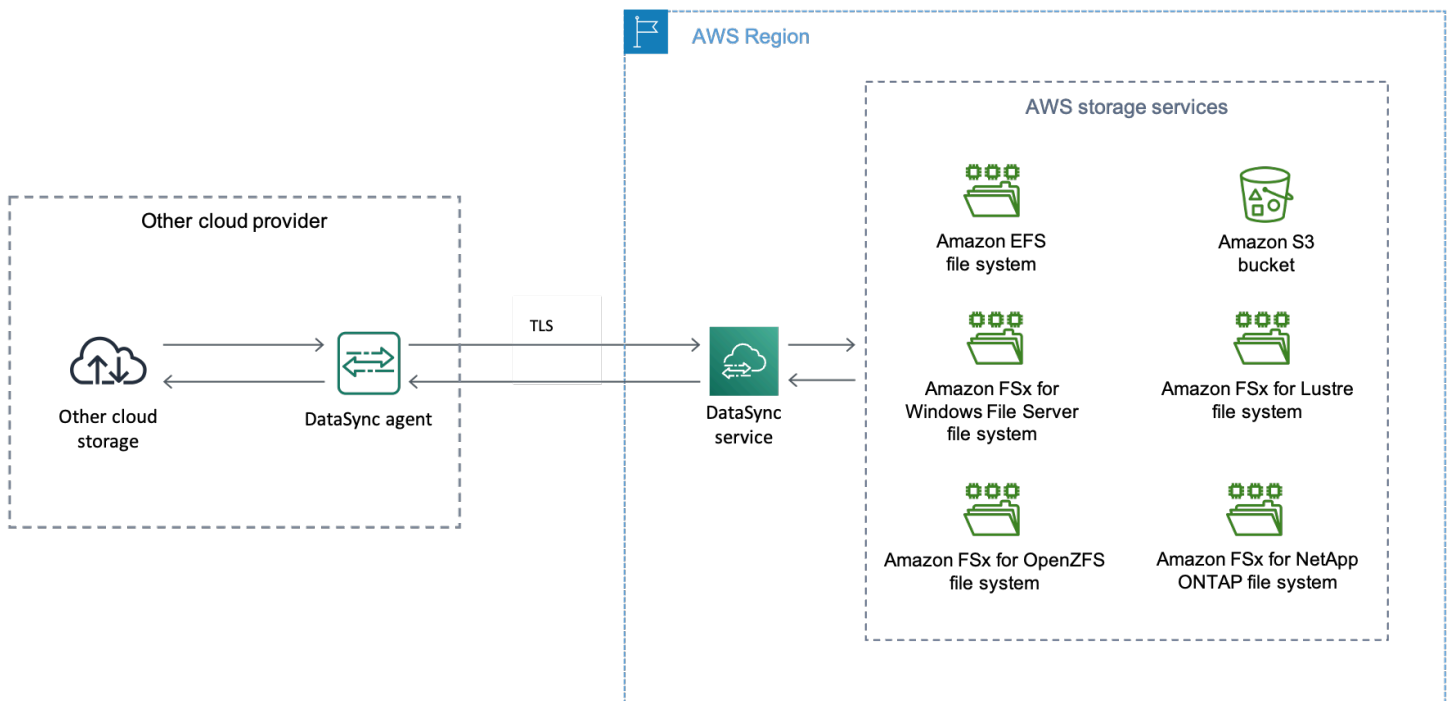
Übertragung zwischen AWS Speicherdiensten und Speichersystemen in anderen Clouds

Mit DataSync können Sie Daten zwischen anderen Cloud-Speichersystemen übertragen und AWS-Services. In diesem Zusammenhang können Cloud-Speichersysteme Folgendes umfassen:

- Selbstverwaltete Speichersysteme, wie z. B. ein NFS-Dateiserver in Ihrer virtuellen privaten Cloud (VPC) innerhalb. AWS
- Speichersysteme oder Dienste, die von einem anderen Cloud-Anbieter gehostet werden. Weitere Informationen finden Sie unter [Übertragung zu oder von einem anderen Cloud-Speicher mit AWS DataSync](#).

DataSync kann Daten mit oder ohne Verwendung eines Agenten in und aus anderen Clouds kopieren. Weitere Informationen darüber, wann Sie einen Agenten einsetzen sollten, finden Sie unter [Benötige ich einen AWS DataSync Agenten?](#) .

Das folgende Diagramm zeigt einen allgemeinen Überblick über die DataSync Übertragung von Daten zwischen AWS Speicherdiensten und einem anderen Cloud-Anbieter.



Konzepte und Terminologie

Machen Sie sich mit den DataSync Übertragungsfunktionen vertraut.

Themen

- [Agent](#)
- [Speicherort](#)
- [Aufgabe](#)

- [Ausführung der Aufgabe](#)

Agent

Ein Agent ist eine Appliance für virtuelle Maschinen (VM), die während einer Übertragung zum Lesen aus dem Speicher und zum Schreiben in den Speicher DataSync verwendet wird. DataSync bietet zwei Arten von Agenten, wobei einer für Aufgaben im Basismodus und ein anderer für Aufgaben im erweiterten Modus zuständig ist. Weitere Informationen zur Auswahl eines Agenten für Ihren Anwendungsfall finden Sie unter [Wählen Sie einen Agenten für Ihren Aufgabenmodus](#).

Sie können einen Agenten in Ihrer Speicherumgebung auf Linux-Kernel-basierten virtuellen Maschinen (KVM) VMware ESXi, Nutanix AHV (unter Verwendung des KVM-Agent-Images) oder Microsoft Hyper-V-Hypervisoren bereitstellen. Für die Speicherung in einer Virtual Private Cloud (VPC) in AWS können Sie einen Agenten als EC2 Amazon-Instance bereitstellen.

Um zu beginnen, siehe [Brauche ich einen AWS DataSync Agenten?](#)

Speicherort

Ein Standort beschreibt, von oder wohin Sie Daten kopieren. Jede DataSync Übertragung (auch als Aufgabe bezeichnet) hat einen Quell- und einen Zielort. Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

Aufgabe

Eine Aufgabe beschreibt eine DataSync Übertragung. Sie identifiziert einen Quell- und einen Zielort sowie Einzelheiten zum Kopieren von Daten zwischen diesen Speicherorten. Sie können auch angeben, wie eine Aufgabe mit Metadaten, gelöschten Dateien und Berechtigungen umgeht.

Ausführung der Aufgabe

Eine Aufgabenausführung ist eine einzelne Ausführung einer DataSync Übertragungsaufgabe. Die Ausführung einer Aufgabe besteht aus mehreren Phasen. Weitere Informationen finden Sie unter [Status der Aufgabenausführung](#).

Wie werden Dateien, Objekte und Verzeichnisse DataSync übertragen

DataSync bereitet Ihre Daten während der [Ausführung einer Aufgabe](#) vor, überträgt und verifiziert sie. Wie diese DataSync Aktionen ausgeführt werden, hängt davon ab, wie Sie Ihre DataSync Aufgabenoptionen konfigurieren, z. B. den [Aufgabenmodus](#). Aufgaben im Basismodus bereiten Ihre Daten sequentiell vor, übertragen und verifizieren Ihre Daten, während Aufgaben im erweiterten Modus diese Aufgaben parallel ausführen.

Themen

- [Wie wird Ihre Datenübertragung DataSync vorbereitet](#)
- [Wie werden deine DataSync Daten übertragen](#)
- [Wie DataSync die Integrität Ihrer Daten überprüft](#)
- [Wie DataSync funktioniert mit geöffneten und gesperrten Dateien](#)
- [Optionen für wiederkehrende Übertragungen](#)

Wie wird Ihre Datenübertragung DataSync vorbereitet

DataSync bereitet Ihre Übertragung standardmäßig vor, indem Ihre Quell- und Zielorte untersucht werden, um festzustellen, was übertragen werden soll. Dazu werden die Inhalte und Metadaten beider Standorte gescannt, um Unterschiede zwischen den beiden zu ermitteln.

Note

Wenn Sie Ihre Aufgabe so konfigurieren, dass [alle Daten übertragen werden](#), ist keine Vorbereitung erforderlich. Wenn Sie Ihre Aufgabe starten, überträgt sie DataSync sofort alles von Ihrer Quelle an Ihr Ziel, ohne Standorte vergleichen zu müssen.

Wie Ihre Übertragung DataSync vorbereitet wird, hängt auch von Ihrem Aufgabenmodus ab:

Verbesserte Modusvorbereitung	Vorbereitung auf den Basismodus
DataSync bereitet Objekte so vor, wie sie am Quellort gefunden wurden. Die Vorbereitung wird während der gesamten Ausführung der	Die Vorbereitung kann je nach Anzahl der Dateien, Objekte oder Verzeichnisse an beiden Speicherorten und der Leistung Ihres Speichers

Verbesserte Modusvorbereitung	Vorbereitung auf den Basismodus
Aufgabe fortgesetzt, bis keine Objekte mehr an der Quelle aufgeführt sind.	nur wenige Minuten, einige Stunden oder sogar länger dauern.
Im Gegensatz zum Basismodus DataSync kann bei jeder Aufgabenausführung eine praktisch unbegrenzte Anzahl von Objekten vorbereitet werden.	Die Elemente, die in Ihrer Quelle und Ihrem Ziel DataSync inventarisiert werden, werden auf Ihre Aufgabenkontingente angerechnet. Diese Kontingente basieren nicht auf der Anzahl der Elemente, die bei jeder Aufgabenausführung DataSync übertragen werden.

DataSync kann bei der Vorbereitung einige Dateien, Objekte und Verzeichnisse überspringen. Die Gründe dafür können von mehreren Faktoren abhängen, z. B. davon, wie Sie Ihre Aufgabe konfigurieren und welche Speichersystemberechtigungen Sie haben. Hier sind einige Beispiele:

- Es gibt eine Datei, die an Ihren Quell- und Zielorten vorhanden ist. Die Datei in der Quelle wurde seit der letzten Ausführung der Aufgabe nicht geändert. Da Sie [nur Daten übertragen, die sich geändert haben](#), wird diese Datei DataSync nicht übertragen, wenn Sie Ihre Aufgabe das nächste Mal ausführen.
- Ein Objekt, das an beiden Speicherorten vorhanden ist, ändert sich in Ihrer Quelle. Wenn Sie Ihre Aufgabe ausführen, wird dieses Objekt in Ihrem Ziel DataSync übersprungen, da Ihre Aufgabe keine [Daten im Ziel überschreibt](#).
- DataSync überspringt ein Objekt an Ihrem Quellspeicherort, das eine [Archivspeicherklasse](#) verwendet und nicht wiederhergestellt wird. Sie müssen ein archiviertes Objekt wiederherstellen, um DataSync es lesen zu können.
- DataSync überspringt eine Datei, ein Objekt oder ein Verzeichnis an Ihrem Quellspeicherort, weil es nicht gelesen werden kann. Wenn dies passiert und nicht zu erwarten ist, überprüfen Sie die Zugriffsberechtigungen Ihres Speichers und stellen Sie sicher, dass gelesen DataSync werden kann, was übersprungen wurde.

Wie werden deine DataSync Daten übertragen

DataSync kopiert Ihre Daten (einschließlich Metadaten) auf der Grundlage Ihrer Aufgabenoptionen von der Quelle zum Ziel. Sie können beispielsweise angeben, welche [Metadaten](#) kopiert werden, bestimmte Dateien [ausschließen](#) und den [DataSync Bandbreitenverbrauch](#) einschränken.

Wie Ihre Daten DataSync übertragen werden, hängt auch von Ihrem Aufgabenmodus ab:

Übertragung im erweiterten Modus	Übertragung im Basismodus
DataSync überträgt jedes Objekt, sobald es vorbereitet ist.	Sobald alle Ihre Daten DataSync vorbereitet sind, beginnt die Übertragung.

DataSync könnte während der Übertragung einige Elemente überspringen. Wenn Sie Ihre Aufgabe so konfigurieren, dass [alle Daten übertragen werden](#), kann dies bei einem Objekt an Ihrem Quellspeicherort passieren, das eine [Archivspeicherklasse](#) verwendet und nicht wiederhergestellt wird.

Wie DataSync wird die Integrität Ihrer Daten überprüft

DataSync führt während einer Übertragung immer Integritätsprüfungen Ihrer Daten durch. DataSync Kann am Ende einer Übertragung auch zusätzliche Prüfungen nur der übertragenen Daten oder des gesamten Datensatzes an beiden Orten durchführen. Weitere Informationen finden Sie unter [Konfiguration, wie AWS DataSync die Datenintegrität überprüft wird](#).

DataSync Berechnet und vergleicht bei der Überprüfung der Datenintegrität die Prüfsumme und die Metadaten der Dateien, Objekte oder Verzeichnisse an Ihren Standorten. Wenn DataSync Unterschiede zwischen den Speicherorten festgestellt werden, schlägt die Überprüfung mit einem Fehler fehl. Beispielsweise könnten Ihnen Fehler wie `Checksum failure`, `Metadata failure` oder `Files were added`, oder angezeigt `Files were removed` werden.

Wie die Überprüfung funktioniert, hängt von Ihrem Aufgabenmodus ab und davon, ob Sie so konfiguriert haben DataSync, dass die Datenintegrität am Ende der Übertragung überprüft wird.

Verifizierung im erweiterten Modus	Überprüfung des Basismodus
DataSync verifiziert jedes Objekt, wenn es an Ihr Ziel übertragen wird.	DataSync Überprüft am Ende Ihrer Übertragung die Integrität Ihrer Daten.
Im erweiterten Modus werden nur übertragene Daten DataSync verifiziert .	Je nachdem, wie Sie die Datenüberprüfung konfigurieren , kann dies bei großen Datensätzen viel Zeit in Anspruch nehmen.

Wie DataSync funktioniert mit geöffneten und gesperrten Dateien

Beachten Sie Folgendes, wenn Sie versuchen, Dateien zu übertragen, die geöffnet (verwendet) oder gesperrt sind:

- Im Allgemeinen DataSync können offene Dateien ohne Einschränkungen übertragen werden.
- Wenn eine Datei geöffnet ist und in die während einer Übertragung geschrieben wird, DataSync kann diese Art von Inkonsistenz während der Überprüfungsphase der Übertragungsaufgabe festgestellt werden. Um die neueste Version der Datei zu erhalten, müssen Sie die Aufgabe erneut ausführen.
- Wenn eine Datei gesperrt ist und der Server sie nicht DataSync öffnen kann, DataSync überspringt er die Datei während der Übertragung und protokolliert einen Fehler.
- DataSync kann Dateien nicht sperren oder entsperren.

Optionen für wiederkehrende Übertragungen

Zusätzlich zu einmaligen Übertragungen DataSync können Daten auch auf wiederkehrender Basis übertragen werden. Zu den Optionen für diese Situationen gehören:

- [Planen](#) Sie, wann Ihre Aufgabe ausgeführt wird.
- Es werden [nur die Daten übertragen, die sich seit der letzten Ausführung der Aufgabe geändert haben](#).
- [Löschen von Daten am Zielort](#), die in der Quelle nicht mehr vorhanden sind.

Erste Schritte mit AWS DataSync

Bevor Sie beginnen AWS DataSync, müssen Sie sich für eine anmelden, AWS-Konto falls Sie noch keine haben. Wir empfehlen außerdem, zu erfahren, wo DataSync Sie Ihre Daten verwenden können und wie viel die Übertragung Ihrer Daten kosten könnte.

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie [https://portal.aws.amazon.com/billing/die Anmeldung](https://portal.aws.amazon.com/billing/die-Anmeldung).
2. Folgen Sie den Online-Anweisungen.

Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu <https://aws.amazon.com/> gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS-Managementkonsole](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung -Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center - Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter [Benutzerzugriff mit der Standardeinstellung konfigurieren](#).AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal](#).

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

Anweisungen hierzu finden Sie unter [Berechtigungssatz erstellen](#) im AWS IAM Identity Center - Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Eine genaue Anleitung finden Sie unter [Gruppen hinzufügen](#) im AWS IAM Identity Center - Benutzerhandbuch.

Erforderliche IAM-Berechtigungen für die Verwendung DataSync

DataSync kann Ihre Daten zu oder von einem Amazon S3 S3-Bucket, Amazon EFS-Dateisystem oder FSx Amazon-Dateisystem übertragen. Um Ihre Daten dorthin zu bringen, wo Sie sie haben möchten, benötigen Sie die richtigen IAM-Berechtigungen, die Ihrer Identität entsprechen. Beispielsweise DataSync benötigt die IAM-Rolle, die Sie mit verwenden, die Erlaubnis, die Amazon S3 S3-Operationen zu verwenden, die für die Übertragung von Daten in einen S3-Bucket erforderlich sind.

Sie können diese Berechtigungen mit IAM-Richtlinien gewähren, die von bereitgestellt werden, AWS oder indem Sie Ihre eigenen Richtlinien erstellen.

Inhalt

- [AWS verwaltete Richtlinien](#)
- [Kundenverwaltete Richtlinien](#)

AWS verwaltete Richtlinien

AWS bietet die folgenden verwalteten Richtlinien für allgemeine DataSync Anwendungsfälle:

- `AWSDataSyncReadOnlyAccess`— Bietet schreibgeschützten Zugriff auf. DataSync
- `AWSDataSyncFullAccess`— Bietet vollen DataSync und minimalen Zugriff auf die zugehörigen Abhängigkeiten.

Weitere Informationen finden Sie unter [AWS verwaltete Richtlinien für AWS DataSync](#).

Kundenverwaltete Richtlinien

Sie können benutzerdefinierte IAM-Richtlinien für die Verwendung mit DataSync erstellen. Weitere Informationen finden Sie unter [Vom Kunden verwaltete IAM-Richtlinien für AWS DataSync](#).

Wo kann ich verwenden? DataSync

Eine Liste der AWS-Regionen DataSync unterstützten Endpunkte finden Sie unter [AWS DataSync Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz

Wie kann ich verwenden? DataSync

Es gibt mehrere Verwendungsmöglichkeiten DataSync:

- [DataSync Konsole](#), die Teil der ist AWS-Managementkonsole.
- [DataSync API](#) oder die [AWS CLI](#) zur programmgesteuerten Konfiguration und Verwaltung. DataSync
- [AWS CloudFormation](#) oder [Terraform](#) zur Bereitstellung Ihrer Ressourcen. DataSync
- [AWS SDKs](#) um Anwendungen zu erstellen, die verwenden. DataSync

Wie viel wird es DataSync kosten?

Informationen zur Erstellung einer individuellen Schätzung anhand der Datenmenge, die Sie übertragen möchten, finden Sie unter [DataSync Preise](#).

Open-Source-Komponenten, die verwendet werden von DataSync

Laden Sie den folgenden Link herunter DataSync, um sich die von verwendeten Open-Source-Komponenten anzusehen:

- [datasync-open-source-components.zip](#)

Brauche ich einen AWS DataSync Agenten?

Für die Verwendung AWS DataSync benötigen Sie möglicherweise einen Agenten. Ein Agent ist eine virtuelle Maschine (VM) -Appliance, die Sie in Ihrer Speicherumgebung für Datenübertragungen einsetzen.

Ob Sie einen Agenten benötigen, hängt von mehreren Faktoren ab, einschließlich der Art des Speichers, zu dem oder von dem Sie Daten übertragen, ob Sie Daten übertragen und zwischen welchen Speicherorten AWS-Regionen Sie Daten übertragen. AWS-Konten Bevor Sie weiterlesen, [überprüfen Sie, ob der Transfer, an dem Sie interessiert sind, DataSync unterstützt](#) wird.

Nachdem Sie festgestellt haben, dass dies Ihr Übertragungsszenario DataSync unterstützt, lesen Sie sich die folgenden Informationen durch, um zu verstehen, ob Sie einen Agenten benötigen.

Situationen, in denen Sie einen DataSync Agenten benötigen

In den meisten Situationen, in denen ein DataSync Agent erforderlich ist, ist Speicher erforderlich, der von Ihnen oder einem anderen Cloud-Anbieter verwaltet wird.

- Übertragung zwischen AWS Speicherdiensten und lokalem Speicher
- Übertragung zwischen Amazon EFS oder Amazon FSx und Speicherung in anderen Clouds
- Übertragung zwischen einigen AWS Speicherdiensten [zwischen AWS-Konten](#) (wenn keiner der Speicherdienste Amazon S3 ist)
- Übertragung zwischen einem Werbespot AWS-Region und einem AWS GovCloud (US) Region , bei dem Quelle und Ziel entweder Amazon EFS oder Amazon sind FSx

Situationen, in denen Sie keinen DataSync Agenten benötigen

Die Situationen, in denen kein Bevollmächtigter erforderlich ist, gelten unabhängig davon, ob Sie innerhalb [derselben](#) Region AWS-Region oder [zwischen verschiedenen Regionen umsteigen](#).

- Übertragung zwischen AWS Speicherdiensten in derselben AWS-Konto
- Übertragung zwischen Amazon S3 und einem anderen AWS Speicherdienst zwischen AWS-Konten
- Übertragung zwischen Amazon S3 und Objektspeicher in anderen Clouds
- Übertragung zwischen einem Werbespot AWS-Region und AWS GovCloud (US) einem, dessen Quelle oder Ziel entweder Amazon S3 ist

Wählen Sie einen Agenten für Ihren Aufgabenmodus

DataSync Aufgaben werden im Basismodus oder im erweiterten Modus ausgeführt. Für Aufgaben im Basismodus ist ein Agent im Basismodus erforderlich. Für Aufgaben im erweiterten Modus ist ein Agent im erweiterten Modus erforderlich.

Der Basismodus unterstützt die Verwendung eines Agenten beim Kopieren an oder von den folgenden Speicherorten:

- NFS

- SMB
- HDFS
- Objektspeicher (einschließlich anderer Clouds)
- Azure-Blob

Der erweiterte Modus unterstützt die Verwendung eines Agenten für Übertragungen von oder zu Amazon S3 mit den folgenden Standorten:

- NFS
- SMB

Weitere Informationen finden Sie unter [Wählen Sie einen Aufgabenmodus für Ihre Datenübertragung](#).

Verwendung mehrerer DataSync Agenten

Während für die meisten Übertragungen nur ein Agent erforderlich ist, kann die Verwendung mehrerer Agenten die Übertragung großer Datensätze mit Millionen von Dateien oder Objekten beschleunigen. In diesen Situationen empfehlen wir, Übertragungsaufgaben parallel auszuführen und dabei einen Agenten pro Aufgabe zu verwenden. Bei diesem Ansatz wird die Übertragungslast auf mehrere Aufgaben verteilt, wobei jede Aufgabe ihren eigenen Agenten verwendet. Es trägt auch dazu bei, den Zeitaufwand DataSync für die Vorbereitung und Übertragung Ihrer Daten zu reduzieren. Weitere Informationen finden Sie unter [Partitionierung großer Datensätze mit mehreren Aufgaben](#).

Eine weitere Option — insbesondere bei Millionen kleiner Dateien — besteht darin, mehrere Agenten mit einem Übertragungsort zu verwenden. Sie können beispielsweise bis zu vier Agenten mit Ihrem lokalen Network File System (NFS) -Dateidienst verbinden. Diese Option kann Ihre Übertragung beschleunigen, obwohl sich die Zeit, die für die Vorbereitung der Übertragung benötigt wird DataSync , nicht ändert.

Denken Sie bei beiden I/O Ansätzen daran, dass diese die Auslastung Ihres Speichers erhöhen und sich auf Ihre Netzwerkbandbreite auswirken können. Weitere Informationen zur Verwendung mehrerer Agenten für Ihre DataSync Übertragungen finden Sie im [AWS Storage-Blog](#).

Wenn Sie darüber nachdenken, mehrere Agenten zu verwenden, denken Sie an Folgendes:

- Einem Standort können bis zu vier Agenten im Basismodus und bis zu vier Agenten im erweiterten Modus zugewiesen werden. Eine Aufgabe, die den Standort verwendet, verwendet nur die Agenten, die dem konfigurierten Aufgabenmodus entsprechen.

- Die Verwendung mehrerer Agenten mit einem Standort bietet keine hohe Verfügbarkeit. Alle Agenten, die einem Standort zugeordnet sind, müssen online sein, bevor Sie mit der Übertragungsaufgabe beginnen können. Wenn einer der Agenten [offline](#) ist, können Sie Ihre Aufgabe nicht ausführen.
- Wenn Sie [einen Virtual Private Cloud \(VPC\) -Dienstendpunkt](#) für die Kommunikation mit dem DataSync Service verwenden, müssen alle Agenten denselben Endpunkt und dasselbe Subnetz verwenden.

Nächste Schritte

- Wenn Sie einen Agenten benötigen, lesen Sie sich die [Agentenanforderungen](#) durch, um zu verstehen, was für Ihre Speicherumgebung sinnvoll ist.
- Wenn Sie für Ihre Übertragung keinen Agenten benötigen, können Sie mit der [Konfiguration Ihrer Übertragung](#) beginnen.

Anforderungen für Agenten AWS DataSync

Bevor Sie einen AWS DataSync Agenten in Ihrer Speicherumgebung [einsetzen](#), stellen Sie sicher, dass Sie den Agent-Hypervisor und die Ressourcenanforderungen verstehen.

Hypervisor-Anforderungen

DataSync Agenten können auf unterstützten Hypervisoren bereitgestellt werden, um die Datenübertragung zu erleichtern.

Note

Agenten im erweiterten Modus unterstützen nur KVM VMware ESXi, Nutanix AHV und. EC2

Sie können einen DataSync Agenten auf den folgenden Hypervisoren ausführen:

- VMware ESXi (Version 7.0 oder 8.0): VMware ESXi ist auf der [Broadcom-Website](#) verfügbar. Sie benötigen außerdem einen VMware vSphere-Client, um eine Verbindung zum Host herzustellen.
- Linux-Kernel-basierte virtuelle Maschine (KVM): Eine kostenlose Open-Source-Virtualisierungstechnologie. KVM ist in den Linux-Versionen 2.6.20 und neuer enthalten. DataSync wurde für die Distributionen CentOS/RHEL 7 und 8, Ubuntu 16.04 LTS und Ubuntu 18.04 LTS

getestet und unterstützt. Andere moderne Linux-Distributionen könnten funktionieren, aber Funktion oder Leistung sind nicht garantiert. Sie müssen die hardwarebeschleunigte Virtualisierung auf Ihrem KVM-Host aktivieren, um Ihren DataSync Agenten einsetzen zu können.

Wir empfehlen diese Option, wenn Sie bereits eine KVM-Umgebung eingerichtet haben und bereits mit der Funktionsweise von KVM vertraut sind.

Die Ausführung von KVM auf Amazon wird EC2 nicht unterstützt und kann nicht für DataSync Agenten verwendet werden.

- Microsoft Hyper-V (Version 2012 R2, 2016 oder 2019): Nur Agenten im Basismodus. Um einen Microsoft Windows-basierten Client-Computer mit dem Host verbinden zu können, benötigen Sie für diese Einrichtung einen Microsoft Hyper-V-Manager.

Der DataSync Agent ist eine virtuelle Maschine (VM) der ersten Generation. Weitere Informationen zu den Unterschieden zwischen Generation 1 und Generation 2 VMs finden Sie unter [Sollte ich eine virtuelle Maschine der Generation 1 oder 2 in Hyper-V erstellen?](#)

- Amazon EC2: DataSync stellt ein Amazon Machine Image (AMI) bereit, das das DataSync Image enthält. Weitere Informationen zu den empfohlenen Instance-Typen finden Sie unter [Anforderungen an EC2 Amazon-Instances](#).

Anforderungen an den Agenten für DataSync Übertragungen

Für DataSync Transfers muss Ihr Agent die folgenden Ressourcenanforderungen erfüllen.

Important

Beachten Sie, dass es sich bei den Agentenanforderungen im Basismodus für die Arbeit mit bis zu 20 Millionen Dateien, Objekten oder Verzeichnissen um allgemeine Richtlinien handelt. Ihr Agent benötigt möglicherweise aufgrund anderer Faktoren mehr Ressourcen, z. B. aufgrund der Anzahl Ihrer Verzeichnisse und der Größe der Objektmetadaten. Beispielsweise ist die m5.2xlarge-Instance für einen EC2 Amazon-Agenten möglicherweise immer noch nicht ausreichend für eine Übertragung von weniger als 20 Millionen Dateien. Agenten im erweiterten Modus haben keine Dateikontingente.

Inhalt

- [Anforderungen an virtuelle Maschinen](#)

- [Anforderungen an EC2 Amazon-Instances](#)

Anforderungen an virtuelle Maschinen

Bei der Bereitstellung eines DataSync Agenten, der sich nicht auf einer EC2 Amazon-Instance befindet, benötigt die Agent-VM die folgenden Ressourcen, je nachdem, ob Sie einen Agenten im Basismodus oder einen Agenten im erweiterten Modus verwenden:

Ressource	Basismodus	Verbesserter Modus
Virtuelle Prozessoren	Vier virtuelle Prozessoren sind der VM zugewiesen	Acht virtuelle Prozessoren, die der VM zugewiesen sind
Festplatt enkapazität	80 GB Festplattenspeicher für die Installation des VM-Images und der Systemdaten	80 GB Festplattenspeicher für die Installation des VM-Images und der Systemdaten
RAM	32 GB RAM wurden der VM für Aufgabenausführungen zugewiesen, die mit bis zu 20 Millionen Dateien, Objekten oder Verzeichnissen arbeiten 64 GB RAM wurden der VM für Aufgabenausführungen zugewiesen, die mit mehr als 20 Millionen Dateien, Objekten oder Verzeichnissen arbeiten	32 GB RAM für die VM

Anforderungen an EC2 Amazon-Instances

Bei der Bereitstellung eines DataSync Agenten auf einer EC2 Amazon-Instance muss die Instance-Größe mindestens 2xlarge sein. Wir empfehlen die Verwendung einer der folgenden Instance-Größen, je nachdem, ob Sie einen Agenten im Basismodus oder einen Agenten im erweiterten Modus verwenden:

Agent im Basismodus	Agent im erweiterten Modus
Verwenden Sie m5.2xlarge für Aufgabenausführungen, die mit bis zu 20 Millionen Dateien, Objekten oder Verzeichnissen arbeiten.	Verwenden Sie m6a.2xlarge unabhängig von der Anzahl der Dateien, Objekte oder Verzeichnisse in Ihrem Datensatz.
Verwenden Sie m5.4xlarge für Aufgabenausführungen, die mit mehr als 20 Millionen Dateien, Objekten oder Verzeichnissen arbeiten.	

Agentenanforderungen für Partitionen AWS-Region

DataSync Agent-Images sind bestimmten [AWS-Region Partitionen](#) zugeordnet. Beispielsweise können Sie standardmäßig keinen Agenten in einem Werbespot herunterladen AWS-Region und ihn dann in einem aktivieren AWS GovCloud (US) Region.

Anforderungen an die Agentenverwaltung

Sobald Sie Ihren DataSync Agenten [aktiviert](#) haben, AWS verwaltet er den Agenten für Sie. Weitere Informationen finden Sie unter [Ihren AWS DataSync Agenten verwalten](#).

Bereitstellen Ihres AWS DataSync Agenten

Bei der Erstellung eines AWS DataSync Agenten besteht der erste Schritt darin, den Agenten in Ihrer Speicherumgebung bereitzustellen. Sie können einen Agenten als virtuelle Maschine (VM) VMware ESXi, Linux-Kernel-basierte virtuelle Maschine (KVM), Nutanix AHV (unter Verwendung des KVM-Images) und Microsoft Hyper-V-Hypervisoren bereitstellen. Sie können einen Agenten auch als EC2 Amazon-Instanz in einer virtuellen privaten Cloud (VPC) innerhalb AWS bereitstellen.

Tip

Bevor Sie beginnen, überprüfen Sie, ob Sie [einen DataSync Agenten benötigen](#).

Bereitstellen Sie Ihren Agenten auf VMware

Sie können einen Agenten von der DataSync Konsole herunterladen und in Ihrer VMware Umgebung bereitstellen.

Bevor Sie beginnen: Stellen Sie sicher, dass Ihre Speicherumgebung einen DataSync Agenten unterstützt. Weitere Informationen finden Sie unter [Anforderungen an virtuelle Maschinen](#).

Um einen Agenten bereitzustellen auf VMware

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich Agents und anschließend Create Agent aus.
3. Wählen Sie für Hypervisor VMWare ESXi die Option Image herunterladen aus.
 - Der Agent im erweiterten Modus wird als .ova Image-Datei heruntergeladen.
 - Der Agent im Basismodus lädt in eine .zip Datei herunter, die die .ova Imagedatei enthält
4. Um die Netzwerklatenz zu minimieren, platzieren Sie den Agenten so nah wie möglich am Speichersystem, das Zugriff DataSync benötigt (möglichst dasselbe lokale Netzwerk). Weitere Informationen finden Sie unter [Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher](#).

Informationen zur Bereitstellung einer .ova Datei auf einem VMware Host finden Sie bei Bedarf in der Dokumentation Ihres Hypervisors.

5. Schalten Sie Ihren Hypervisor ein, melden Sie sich bei der Agenten-VM an und rufen Sie die IP-Adresse des Agenten ab. Diese IP-Adresse benötigen Sie, um den Agenten zu aktivieren.

Die Standardanmeldedaten der Agent-VM sind Login **admin** und Passwort **password**. Ändern Sie bei Bedarf das Passwort über die [lokale Konsole der VM](#).

Nächster Schritt: [Wählen Sie einen Service-Endpunkt für Ihren Agenten AWS DataSync](#)

Bereitstellen Ihres Agenten auf KVM

Sie können einen Agenten von der DataSync Konsole herunterladen und ihn in Ihrer KVM-Umgebung bereitstellen.

Bevor Sie beginnen: Stellen Sie sicher, dass Ihre Speicherumgebung einen DataSync Agenten unterstützt. Weitere Informationen finden Sie unter [Anforderungen an virtuelle Maschinen](#).

So stellen Sie einen Agenten auf KVM bereit

1. Öffnen Sie die AWS DataSync Konsole unter. <https://console.aws.amazon.com/datasync/>
2. Wählen Sie im linken Navigationsbereich Agents und anschließend Create Agent aus.
3. Wählen Sie für Hypervisor die Option Kernel-based Virtual Machine (KVM) und dann Image herunterladen aus.
 - Der Agent im erweiterten Modus wird als Image-Datei heruntergeladen. .qcow2
 - Der Agent im Basismodus lädt in eine .zip Datei herunter, die die .qcow2 Imagedatei enthält
4. Um die Netzwerklatenz zu minimieren, platzieren Sie den Agenten so nah wie möglich am Speichersystem, das Zugriff DataSync benötigt (möglichst dasselbe lokale Netzwerk). Weitere Informationen finden Sie unter [Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher](#).
5. Führen Sie den folgenden Befehl aus, um Ihr .qcow2 Image zu installieren.

```
virt-install \
  --name "datasync" \
  --description "DataSync agent" \
  --os-type=generic \
  --ram=32768 \
  --vcpus=4 \
  --disk path=datasync-yyyyymmdd-x86_64.qcow2,bus=virtio,size=80 \
  --network default,model=virtio \
  --graphics none \
  --virt-type kvm \
  --import
```

Informationen zur Verwaltung dieser VM und Ihres KVM-Hosts finden Sie in der Dokumentation Ihres Hypervisors.

6. Starten Sie Ihren Hypervisor, melden Sie sich bei Ihrer VM an und bestimmen Sie die IP-Adresse des Agenten. Diese IP-Adresse benötigen Sie, um den Agenten zu aktivieren.

Die Standardanmeldedaten der Agent-VM lauten Login **admin** und Passwort. **password** Ändern Sie bei Bedarf das Passwort über die [lokale Konsole der VM](#).

Nächster Schritt: [Wählen Sie einen Service-Endpunkt für Ihren Agenten AWS DataSync](#)

Bereitstellen Ihres Agenten im Basismodus auf Microsoft Hyper-V

Sie können einen Agenten im Basismodus von der DataSync Konsole herunterladen und ihn in Ihrer Microsoft Hyper-V-Umgebung bereitstellen.

Bevor Sie beginnen: Stellen Sie sicher, dass Ihre Speicherumgebung einen DataSync Agenten unterstützt. Weitere Informationen finden Sie unter [Anforderungen an virtuelle Maschinen](#).

So stellen Sie einen Agenten im Basismodus auf Hyper-V bereit

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>
2. Wählen Sie im linken Navigationsbereich Agents und anschließend Create Agent aus.
3. Wählen Sie für Hypervisor Microsoft Hyper-V und dann Bild herunterladen aus.

Der Agent lädt eine Datei herunter, die eine .zip Bilddatei enthält. .vhdx

4. Um die Netzwerklatenz zu minimieren, platzieren Sie den Agenten so nah wie möglich am Speichersystem, das Zugriff DataSync benötigt (möglichst dasselbe lokale Netzwerk). Weitere Informationen finden Sie unter [Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher](#).

Informationen zur Bereitstellung einer .vhdx Datei auf einem Hyper-V-Host finden Sie bei Bedarf in der Dokumentation Ihres Hypervisors.

Warning

Möglicherweise stellen Sie eine schlechte Netzwerkleistung fest, wenn Sie Virtual Machine Queue (VMQ) auf einem Hyper-V-Host aktivieren, der einen Broadcom-Netzwerkadapter verwendet. Informationen zu einer Problemumgehung finden Sie in der [Microsoft-Dokumentation](#).

5. Starten Sie Ihren Hypervisor, melden Sie sich bei Ihrer VM an und bestimmen Sie die IP-Adresse des Agenten. Diese IP-Adresse benötigen Sie, um den Agenten zu aktivieren.

Die Standardanmeldedaten der Agent-VM sind Login **admin** und Passwort **password**. Ändern Sie bei Bedarf das Passwort über die [lokale Konsole der VM](#).

Nächster Schritt: [Wählen Sie einen Service-Endpunkt für Ihren Agenten AWS DataSync](#)

Bereitstellung Ihres EC2 Amazon-Agenten

Sie können einen DataSync Agenten als EC2 Amazon-Instance einsetzen, wenn Sie Daten übertragen zwischen:

- Ein selbstverwaltetes Cloud-Speichersystem (z. B. ein NFS-Dateiserver in AWS) und ein AWS Speicherdienst.
- Ein Cloud-Speicheranbieter (wie Microsoft Azure Blob Storage oder Google Cloud Storage) und ein AWS Speicherdienst, der den Basismodus verwendet.
- Ein S3-Bucket in einem kommerziellen AWS-Region und ein S3-Bucket in einem AWS GovCloud (US) Region.
- [Amazon S3 aktiviert AWS Outposts](#) und ein AWS Speicherservice im Basismodus.

Warning

Aufgrund der erhöhten Netzwerklatenz empfehlen wir nicht, einen EC2 Amazon-Agenten mit lokalem Speicher zu verwenden. Stellen Sie den Agenten stattdessen als virtuelle KVM-VMware, KVM- oder Hyper-V-Maschine in Ihrem Rechenzentrum so nah wie möglich an Ihrem lokalen Speicher bereit.

EC2 Bereitstellen Ihres Agenten

Um das Agent-AMI für Ihr auszuwählen AWS-Region

1. Öffnen Sie ein Terminal und kopieren Sie den folgenden AWS CLI Befehl, um die neueste DataSync Amazon Machine Image (AMI) -ID für die Region zu erhalten, in der Sie Ihren EC2 Amazon-Agenten einsetzen möchten.

Agenten im Basismodus

```
aws ssm get-parameter --name /aws/service/datasync/ami --region your-region
```

Agenten im erweiterten Modus

```
aws ssm get-parameter --name /aws/service/datasync/ami/v3 --region your-region
```

2. Führen Sie den Befehl aus. Notieren Sie sich in der Ausgabe die "Value" Eigenschaft mit der DataSync AMI-ID.

Example Beispielbefehl und Ausgabe

```
aws ssm get-parameter --name /aws/service/datasync/ami --region us-east-1

{
  "Parameter": {
    "Name": "/aws/service/datasync/ami",
    "Type": "String",
    "Value": "ami-1234567890abcdef0",
    "Version": 6,
    "LastModifiedDate": 1569946277.996,
    "ARN": "arn:aws:ssm:us-east-1::parameter/aws/service/datasync/ami"
  }
}
```

So setzen Sie Ihren EC2 Amazon-Agenten ein

Tip

Um Gebühren für die Übertragung zwischen Availability Zones zu vermeiden, sollten Sie Ihren Agenten so einsetzen, dass er keinen Netzwerkverkehr zwischen Availability Zones benötigt. (Weitere Informationen zu den Datenübertragungspreisen für alle AWS-Regionen finden Sie unter [Amazon EC2 Data Transfer — Preise](#).)

Stellen Sie Ihren Agenten beispielsweise in der Availability Zone bereit, in der sich Ihr selbstverwaltetes Cloud-Speichersystem befindet.

1. Kopieren Sie die folgende URL:

```
https://console.aws.amazon.com/ec2/v2/home?region=agent-region#LaunchInstanceWizard:ami=ami-id
```

- *agent-region* Ersetzen Sie es durch die Region, in der Sie Ihren Agenten einsetzen möchten.
- *ami-id* Ersetzen Sie durch die DataSync AMI-ID, die Sie erhalten haben.

2. Fügen Sie die URL in einen Browser ein.

Die Startseite der EC2 Amazon-Instance AWS-Managementkonsole wird angezeigt.

3. Wählen Sie unter Instance-Typ eine der [empfohlenen EC2 Amazon-Instances](#) für aus DataSync.
4. Wählen Sie für key pair ein vorhandenes Schlüsselpaar aus, oder erstellen Sie ein neues.
5. Wählen Sie für Netzwerkeinstellungen die Option Bearbeiten und gehen Sie dann wie folgt vor:
 - a. Wählen Sie für VPC eine VPC aus, in der Sie Ihren Agenten bereitstellen möchten.
 - b. Wählen Sie für Auto-Assign Public IP aus, ob Ihr Agent vom öffentlichen Internet aus zugänglich sein soll.

Sie verwenden die öffentliche oder private IP-Adresse der Instanz später, um Ihren Agenten zu aktivieren.

- c. Erstellen Sie für Firewall (Sicherheitsgruppen) eine Sicherheitsgruppe, die Folgendes tut, oder wählen Sie eine aus:
 - Lässt bei Bedarf eingehenden Datenverkehr zur EC2 Amazon-Instance auf Port 80 (HTTP) zu. Für einige Optionen zum [Abrufen eines Agenten-Aktivierungsschlüssels](#) ist diese Verbindung erforderlich.
 - Ermöglicht eingehenden und ausgehenden Verkehr zwischen der EC2 Amazon-Instance und dem Speichersystem, zu dem Sie Daten übertragen oder von dem Sie Daten übertragen. Weitere Informationen finden Sie unter [Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher](#).

 Note

Abhängig von der Art des [Service-Endpunkts](#), den Ihr Agent verwendet, müssen zusätzliche Ports konfiguriert werden.

6. (Empfohlen) Um die Leistung bei der Übertragung von einem cloudbasierten Dateisystem zu erhöhen, erweitern Sie Erweiterte Details und wählen Sie einen Wert für die Platzierungsgruppe aus, in der sich Ihr Speicher befindet.
7. Wählen Sie Launch instance, um Ihre EC2 Amazon-Instance zu starten.
8. Sobald Ihr Instance-Status Running lautet, wählen Sie die Instance aus.

9. Wenn Sie Ihre Instance so konfiguriert haben, dass sie vom öffentlichen Internet aus zugänglich ist, notieren Sie sich die öffentliche IP-Adresse der Instance. Falls nicht, notieren Sie sich die private IP-Adresse.

Sie benötigen diese IP-Adresse, wenn [Sie Ihren Agenten aktivieren](#).

Beispiele: Bereitstellung Ihres EC2 Agenten in einem AWS-Region

Die folgenden Anleitungen können bei häufigen Szenarien helfen, wenn Sie einen DataSync Agenten in einem einsetzen AWS-Region.

Themen

- [Bereitstellen Ihres Agenten im Basismodus für Übertragungen zwischen Cloud-Speicher und AWS Speicherdiensten](#)
- [Bereitstellung Ihres Agenten im Basismodus für Übertragungen zwischen Amazon S3 und AWS Dateisystemen](#)

Bereitstellen Ihres Agenten im Basismodus für Übertragungen zwischen Cloud-Speicher und AWS Speicherdiensten

Um Daten zwischen oder zwischen AWS-Konten Cloud-Speichersystemen zu übertragen, muss sich der DataSync Agent im selben AWS-Region und AWS-Konto dort, wo sich das Quelldateisystem befindet, befinden. Diese Art der Übertragung umfasst Folgendes:

- Übertragungen zwischen Amazon EFS oder Amazon FSx zum AWS Speicher in einem anderen AWS-Konto.
- Übertragungen von selbstverwalteten Dateisystemen zu AWS Speicherdiensten.

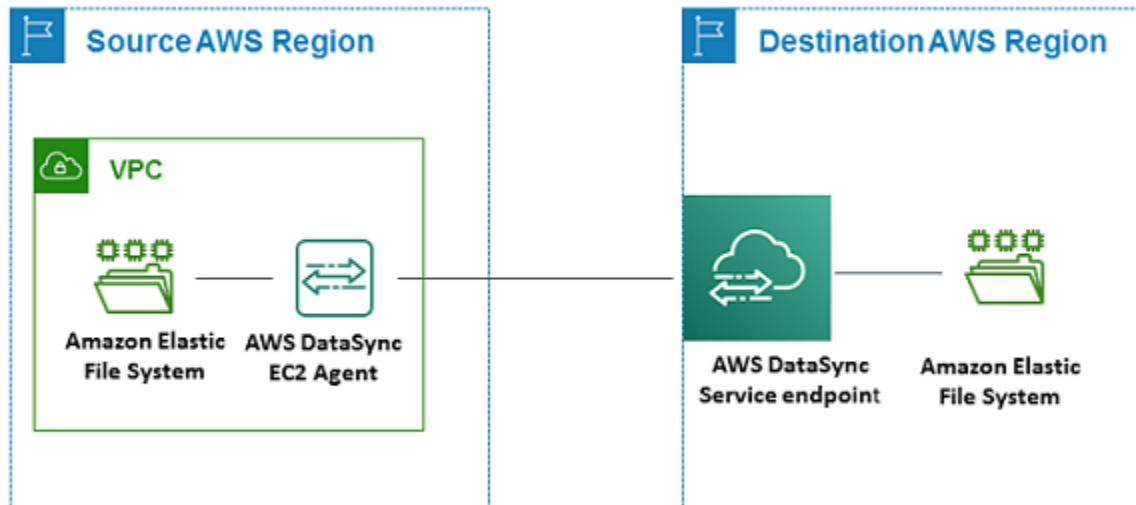
 Important

Stellen Sie Ihren Agenten so ein, dass er keinen Netzwerkverkehr zwischen Availability Zones benötigt (um Gebühren für diesen Verkehr zu vermeiden).

- Um auf Ihr Amazon EFS- oder FSx Windows File Server-Dateisystem zuzugreifen, stellen Sie den Agenten in einer Availability Zone bereit, die ein Mount-Ziel für Ihr Dateisystem hat.
- Bei selbstverwalteten Dateisystemen stellen Sie den Agenten in der Availability Zone bereit, in der sich Ihr Dateisystem befindet.

Weitere Informationen zu den Datenübertragungspreisen für alle AWS-Regionen finden Sie unter [Amazon EC2 On-Demand-Preise](#).

Das folgende Diagramm zeigt beispielsweise eine allgemeine Ansicht der DataSync Architektur für die Übertragung von Daten vom Cloud-internen Network File System (NFS) zu Cloud-NFS oder Amazon S3.



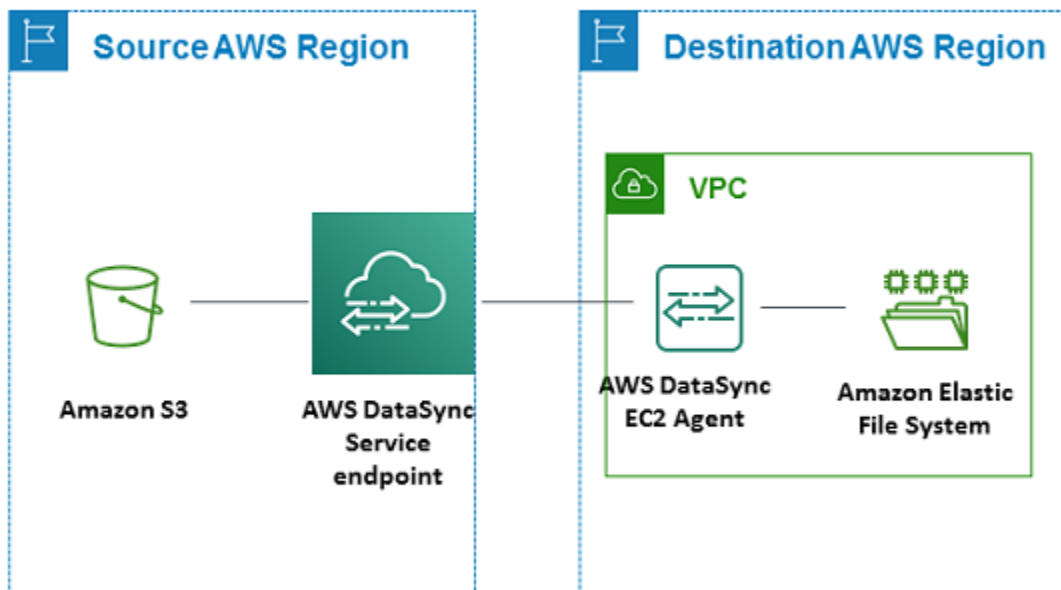
Beachten Sie bei der Übertragung zwischen AWS Speicherdiensten Folgendes: AWS-Konten

- Wenn Sie zwischen Amazon EFS-Dateisystemen oder FSx Amazon-Dateisystemen mithilfe des NFS-Protokolls übertragen, konfigurieren Sie Ihr Quelldateisystem als [NFS-Speicherort](#).
- Wenn Sie mithilfe des SMB-Protokolls zwischen FSx Amazon-Dateisystemen übertragen, konfigurieren Sie Ihr Quelldateisystem als [SMB-Speicherort](#).

Bereitstellung Ihres Agenten im Basismodus für Übertragungen zwischen Amazon S3 und AWS Dateisystemen

Das folgende Diagramm bietet einen allgemeinen Überblick über die DataSync Architektur für die Übertragung von Daten von Amazon S3 in ein AWS Dateisystem wie Amazon EFS oder Amazon FSx. Sie können diese Architektur verwenden, um Daten von einem AWS-Konto zum anderen

zu übertragen oder um Daten von Amazon S3 in ein selbstverwaltetes In-Cloud-Dateisystem zu übertragen.



Bereitstellen Ihres Agenten im Basismodus auf AWS Outposts

Sie können eine DataSync EC2 Amazon-Instance auf Ihrem Outpost starten. Weitere Informationen zum Starten eines AMI auf AWS Outposts finden Sie unter [Starten einer Instance auf Ihrem Outpost](#) im AWS Outposts Benutzerhandbuch.

Wenn Sie auf Outposts auf Amazon S3 zugreifen möchten, müssen Sie einen Agenten im Basismodus verwenden und ihn in einer VPC starten, die Zugriff auf Ihren Amazon S3 S3-Zugangspunkt hat, und den Agenten in der übergeordneten Region des Outposts aktivieren. DataSync Der Agent muss auch in der Lage sein, für den Bucket zum Endpunkt Amazon S3 on Outposts weiterzuleiten. Weitere Informationen zur Arbeit mit Amazon S3 auf Outposts-Endpunkten finden Sie unter [Arbeiten mit Amazon S3 auf Outposts](#) im Amazon S3 S3-Benutzerhandbuch.

Wählen Sie einen Service-Endpunkt für Ihren Agenten AWS DataSync

Ein [Service-Endpunkt](#) ist die Art und Weise, wie Ihr AWS DataSync [Agent mit dem Service kommuniziert](#). DataSync DataSync unterstützt die folgenden Arten von Dienstendpunkten:

- Endpunkt des öffentlichen Dienstes — Daten werden über das öffentliche Internet gesendet.

- FIPS-Dienstendpunkt (Federal Information Processing Standard) — Daten werden mithilfe von FIPS-konformen Prozessen über das öffentliche Internet übertragen.
- Service-Endpunkt der Virtual Private Cloud (VPC) — Daten werden über Ihre VPC statt über das öffentliche Internet gesendet, wodurch die Sicherheit Ihrer übertragenen Daten erhöht wird.
- FIPS-VPC-Serviceendpunkt — Daten werden mithilfe von FIPS-konformen Prozessen über Ihre VPC gesendet.

[Sie benötigen einen Service-Endpunkt, um Ihren Agenten zu aktivieren.](#) Beachten Sie bei der Auswahl eines Service-Endpunkts Folgendes:

- Ein Agent kann nur einen Endpunkttyp verwenden. Wenn Sie Daten mit unterschiedlichen Endpunkttypen übertragen müssen, erstellen Sie für jeden Typ einen Agenten.
- Wie Sie [Ihr Speichernetzwerk verbinden, AWS bestimmt](#), welche Service-Endpunkte Sie verwenden können.

Auswahl eines Endpunkts für öffentliche Dienste

Wenn Sie einen öffentlichen Dienstendpunkt verwenden, erfolgt die gesamte Kommunikation zwischen Ihrem DataSync Agenten und dem DataSync Dienst über das öffentliche Internet.

1. Ermitteln Sie den [Endpunkt des DataSync öffentlichen Dienstes](#), den Sie verwenden möchten.
2. [Konfigurieren Sie Ihr Netzwerk](#) so, dass der für die Nutzung von Endpunkten des DataSync öffentlichen Dienstes erforderliche Datenverkehr zugelassen wird.

Nächster Schritt: [Ihren AWS DataSync Agenten aktivieren](#)

Auswahl eines FIPS-Serviceendpunkts

DataSync stellt einige Dienstendpunkte bereit, die FIPS-konform sind. Weitere Informationen finden Sie unter [FIPS-Endpunkte](#) in der. Allgemeine AWS-Referenz

1. Ermitteln Sie den DataSync [FIPS-Dienstendpunkt](#), den Sie verwenden möchten.
2. [Konfigurieren Sie Ihr Netzwerk](#) so, dass der für die Verwendung von DataSync FIPS-Dienstendpunkten erforderliche Datenverkehr zugelassen wird.

Nächster Schritt: [Ihren AWS DataSync Agenten aktivieren](#)

Auswahl eines VPC-Serviceendpunkts

Wenn Sie einen VPC-Serviceendpunkt verwenden, werden Ihre Daten nicht über das öffentliche Internet übertragen. DataSync überträgt stattdessen Daten über eine VPC, die auf dem Amazon VPC-Service basiert.

Inhalt

- [So arbeiten DataSync Agenten mit VPC-Serviceendpunkten](#)
- [DataSync Einschränkungen bei VPCs](#)
- [Erstellen eines VPC-Serviceendpunkts für DataSync](#)

So arbeiten DataSync Agenten mit VPC-Serviceendpunkten

VPC-Dienstendpunkte werden von bereitgestellt. AWS PrivateLink Mit diesen Arten von Endpunkten können Sie eine private Verbindung AWS-Services zu Ihrer unterstützten VPC herstellen. Wenn Sie einen VPC-Serviceendpunkt mit verwenden DataSync, verbleibt die gesamte Kommunikation zwischen Ihrem DataSync Agenten und dem DataSync Service in Ihrer VPC.

Der VPC-Dienstendpunkt (zusammen mit den [Netzwerkschnittstellen](#), die für den Datenübertragungsverkehr DataSync erstellt werden) verwendet private IP-Adressen, auf die nur innerhalb Ihrer VPC zugegriffen werden kann. Weitere Informationen finden Sie unter [Ihr Netzwerk für AWS DataSync Übertragungen verbinden](#).

DataSync Einschränkungen bei VPCs

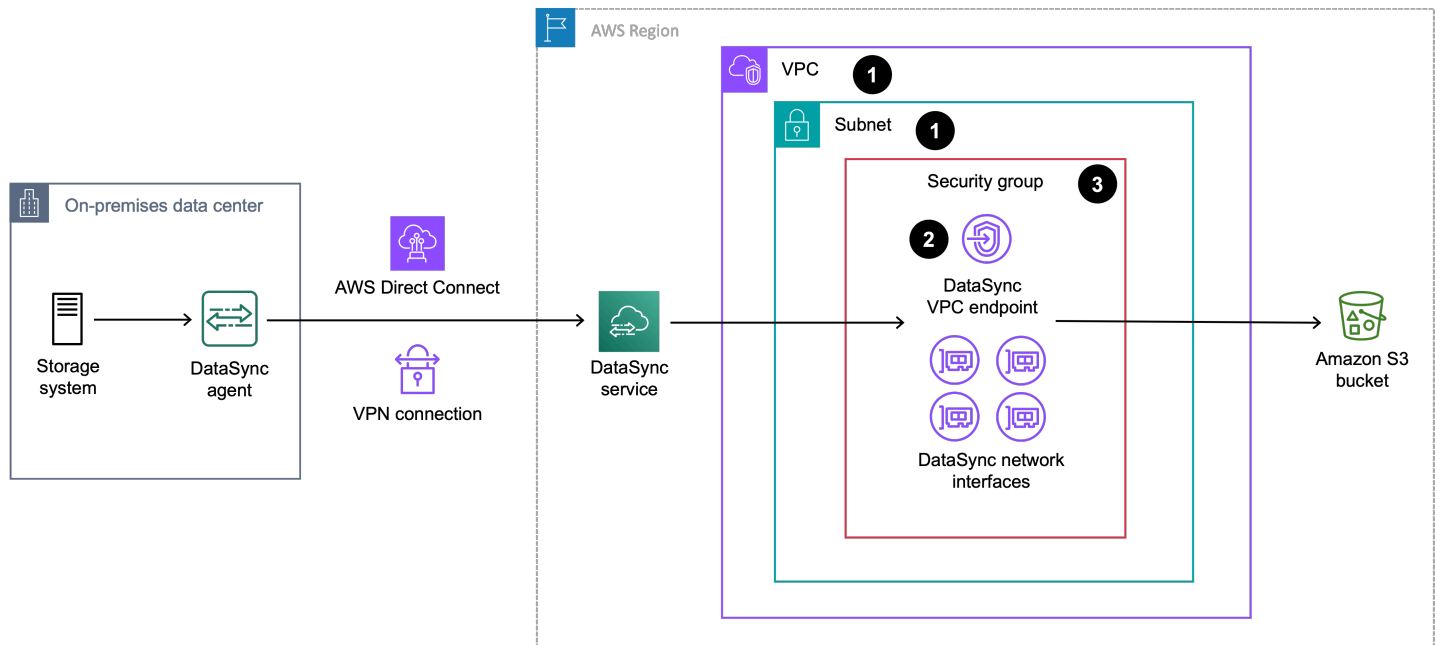
- VPCs das Sie mit verwenden, DataSync muss über eine Standardmietdauer verfügen. VPCs mit Dedicated Tenancy werden nicht unterstützt.
- DataSync unterstützt [Shared VPCs](#) nicht.

Erstellen eines VPC-Serviceendpunkts für DataSync

Sie erstellen einen VPC-Serviceendpunkt für DataSync in einer VPC, die Sie verwalten. Ihr Service-Endpunkt, Ihre VPC und Ihr DataSync Agent müssen zu demselben AWS-Konto gehören.

Das folgende Diagramm zeigt ein Beispiel für die DataSync Verwendung eines VPC-Serviceendpunkts für die Übertragung von einem lokalen Speichersystem zu einem Amazon

S3 S3-Bucket. Die nummerierten Callouts entsprechen den Schritten zum Erstellen eines VPC-Dienstendpunkts.



So erstellen Sie einen VPC-Serviceendpunkt für DataSync

1. [Erstellen](#) oder bestimmen Sie eine VPC und ein Subnetz, in denen Sie Ihren VPC-Serviceendpunkt erstellen möchten.

Wenn Sie zu oder von einem externen Speicher übertragen AWS, sollte sich die VPC auf diese Speicherumgebung erstrecken (Ihre Speicherumgebung könnte beispielsweise ein Rechenzentrum sein, in dem sich Ihr lokaler NFS-Dateiserver befindet). Sie können dies tun, indem Sie Routing-Regeln über [Direct Connect](#) oder VPN verwenden.

2. Erstellen Sie einen DataSync VPC-Dienstendpunkt, indem Sie wie folgt vorgehen:
 - a. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
 - b. Wählen Sie im linken Navigationsbereich Endpoints und anschließend Create Endpoint aus.
 - c. Wählen Sie für Servicekategorie die Option AWS-Services aus.
 - d. Suchen Sie unter Dienste nach dem Endpunkt für den, in dem Sie sich befinden AWS-Region , **datasync** und wählen Sie ihn aus (z. B. `com.amazonaws.us-east-1.datasync` oder `com.amazonaws.us-east-1.datasync-fips`).
 - e. Wählen Sie für VPC die VPC aus, in der Sie den VPC-Serviceendpunkt erstellen möchten.
 - f. Erweitern Sie Zusätzliche Einstellungen und deaktivieren Sie das Kontrollkästchen Privaten DNS-Namen aktivieren, um diese Einstellung zu deaktivieren.

Wir empfehlen, diese Einstellung zu deaktivieren, falls Sie Agenten in derselben VPC haben, die einen öffentlichen Dienstendpunkt verwenden müssen. Ein Agent kann über das Netzwerk keinen [Endpunkt eines öffentlichen Dienstes](#) erreichen, wenn diese Einstellung aktiviert ist.

- g. Wählen Sie für Subnetz das Subnetz aus, in dem Sie den VPC-Dienstendpunkt erstellen möchten. Notieren Sie sich den Subnetz-ARN (Sie benötigen ihn, wenn Sie Ihren Agenten aktivieren).
 - h. Wählen Sie Endpunkt erstellen aus. Notieren Sie sich die Endpunkt-ID (Sie benötigen diese, wenn Sie Ihren Agenten aktivieren).
3. Konfigurieren Sie in Ihrer VPC eine [Sicherheitsgruppe](#), die den für die Verwendung von DataSync [VPC-Dienstendpunkten](#) erforderlichen Datenverkehr zulässt. Notieren Sie sich den ARN der Sicherheitsgruppe (Sie benötigen ihn, wenn Sie Ihren Agenten aktivieren).

Die Sicherheitsgruppe muss es Ihrem Agenten ermöglichen, eine Verbindung mit den privaten IP-Adressen des VPC-Dienstendpunkts und Ihren [Netzwerkschnittstellen](#) herzustellen (die bei der Erstellung Ihrer Aufgabe erstellt werden).

Nächster Schritt: [Ihren AWS DataSync Agenten aktivieren](#)

Ihren AWS DataSync Agenten aktivieren

Um die Erstellung Ihres AWS DataSync Agenten abzuschließen, müssen Sie ihn aktivieren. In diesem Schritt wird der Agent Ihrem zugeordnet AWS-Konto.

Note

Sie können einen Agenten nicht in mehr als einem AWS-Konto und AWS-Region gleichzeitig aktivieren.

Voraussetzungen

Um Ihren DataSync Agenten zu aktivieren, stellen Sie sicher, dass Sie über die folgenden Informationen verfügen:

- Der [DataSync Service-Endpunkt](#), mit dem Sie Ihren Agenten aktivieren.

Wenn Sie einen VPC-Serviceendpoint verwenden, benötigen Sie diese Informationen:

- Die VPC-Dienstendpunkt-ID.
- Das Subnetz, in dem sich Ihr VPC-Dienstendpunkt befindet.
- Die Sicherheitsgruppe, die den für die Verwendung von DataSync [VPC-Dienstendpunkten](#) erforderlichen Datenverkehr zulässt.
- Die IP-Adresse oder der Domainname Ihres Agenten.

Wie Sie das herausfinden, hängt von der Art des Agenten ab, den Sie [einsetzen](#). Wenn es sich bei Ihrem Agenten beispielsweise um eine EC2 Amazon-Instance handelt, finden Sie dessen IP-Adresse auf der EC2 Amazon-Konsole auf der Seite der Instance.

Note

Verwenden Sie für FIPS-VPC-Endpunkte die AWS CLI API oder DataSync

Einen Aktivierungsschlüssel erhalten

Sie können einen Aktivierungsschlüssel für Ihren eingesetzten DataSync Agenten auf verschiedene Arten erhalten. Für einige Optionen ist Zugriff auf Ihren Agenten über Port 80 (HTTP) erforderlich. Wenn Sie eine dieser Optionen verwenden, DataSync wird der Port geschlossen, sobald Sie den Agenten aktiviert haben.

Note

Agenten-Aktivierungsschlüssel laufen in 30 Minuten ab, wenn sie nicht verwendet werden.

DataSync console

Wenn [Sie Ihren Agenten in der DataSync Konsole aktivieren](#), DataSync können Sie den Aktivierungsschlüssel für Sie abrufen, indem Sie die Option Automatisch den Aktivierungsschlüssel von Ihrem Agenten abrufen verwenden.

Um diese Option verwenden zu können, muss Ihr Browser Ihren Agenten über Port 80 erreichen können.

Agent local console

Im Gegensatz zu den anderen Optionen zum Abrufen eines Aktivierungsschlüssels muss Ihr Agent für diese Option nicht über Port 80 erreichbar sein.

1. Melden Sie sich bei der [lokalen Konsole](#) Ihrer Agenten-VM oder EC2 Amazon-Instance an.
2. Geben Sie im Hauptmenü AWS DataSync Aktivierung — Konfiguration die Eingabetaste ein, **0** um einen Aktivierungsschlüssel zu erhalten.
3. Geben Sie den ein AWS-Region , in dem Sie Ihren Agenten aktivieren.
4. Geben Sie den Typ des Service-Endpunkts ein, den Ihr Agent verwendet.
5. Kopieren Sie den angezeigten Aktivierungsschlüssel.

Beispiel: F0EFT-7FPPR-GG7MC-3I9R3-27DOH

Sie geben diesen Schlüssel bei der [Aktivierung Ihres Agenten](#) an.

CLI

Mit Standard-Unix-Tools können Sie eine `curl` Anfrage an die IP-Adresse Ihres Agenten senden, um dessen Aktivierungsschlüssel zu erhalten.

Um diese Option nutzen zu können, muss Ihr Client Ihren Agenten über Port 80 erreichen können. Sie können den folgenden Befehl ausführen, um dies zu überprüfen:

```
nc -vz agent-ip-address 80
```

Sobald Sie bestätigt haben, dass Sie den Agenten erreichen können, führen Sie je nach Art des verwendeten Dienstendpunkts einen der folgenden Befehle aus:

- Endpunkte des öffentlichen Dienstes:

```
curl "http://agent-ip-address?gatewayType=SYNC&activationRegion=your-region&no_redirect"
```

- Endpunkte des FIPS-Dienstes:

```
curl "http://agent-ip-address?gatewayType=SYNC&activationRegion=your-region&endpointType=FIPS&no_redirect"
```

- VPC-Dienstendpunkte:

```
curl "http://agent-ip-address?gatewayType=SYNC&activationRegion=your-region&privateLinkEndpoint=vpc-endpoint-ip-address&endpointType=PRIVATE_LINK&no_redirect"
```

- FIPS-VPC-Dienstendpunkte:

```
curl "http://agent-ip-address?gatewayType=SYNC&activationRegion=your-region&privateLinkEndpoint=vpc-endpoint-ip-address&endpointType=FIPS_PRIVATE_LINK&no_redirect"
```

 Note

Um das zu finden *vpc-endpoint-ip-address*, öffnen Sie die [Amazon VPC-Konsole](#), wählen Sie Endpoints und dann Ihren DataSync VPC-Service-Endpoint aus. Suchen Sie auf der Registerkarte Subnetze die IP-Adresse für das Subnetz Ihres [VPC-Dienstendpunkts](#). Dies ist die IP-Adresse des Endpunkts.

Dieser Befehl gibt einen Aktivierungsschlüssel zurück. Beispiel:

F0EFT-7FPPR-GG7MC-3I9R3-27D0H

Sie geben diesen Schlüssel bei der [Aktivierung Ihres Agenten](#) an.

Ihren Agenten aktivieren

Sie haben mehrere Möglichkeiten, Ihren DataSync Agenten zu aktivieren. AWS [Verwaltet den Agenten nach der](#) Aktivierung für Sie.

DataSync console

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich Agents und anschließend Create Agent aus.
3. Gehen Sie im Abschnitt Dienstendpunkt wie folgt vor, um den Service-Endpoint für Ihren Agenten anzugeben:

- Wählen Sie für einen öffentlichen Dienstendpunkt die Option Öffentliche Dienstendpunkte in ***your current AWS-Region*** aus.
 - Wählen Sie für einen FIPS-Dienstendpunkt die Option FIPS-Dienstendpunkte in aus. ***your current AWS-Region***
 - Gehen Sie für einen VPC-Dienstendpunkt wie folgt vor:
 - Wählen Sie VPC-Endpunkte mit. AWS PrivateLink
 - Wählen Sie für VPC-Endpunkt den VPC-Serviceendpunkt aus, den Ihr Agent verwenden soll.
 - Wählen Sie für Subnetz das Subnetz aus, in dem sich Ihr VPC-Dienstendpunkt befindet.
 - Wählen Sie für Sicherheitsgruppe die Sicherheitsgruppe aus, die den für die Verwendung von DataSync [VPC-Dienstendpunkten](#) erforderlichen Datenverkehr zulässt.
4. Führen Sie im Abschnitt Aktivierungsschlüssel einen der folgenden Schritte aus, um den Aktivierungsschlüssel Ihres Agenten anzugeben:
- Wählen Sie Automatisch den Aktivierungsschlüssel von Ihrem Agenten abrufen für DataSync , um den Schlüssel für Sie zu erhalten.
 - Geben Sie als Agentenadresse die IP-Adresse oder den Domainnamen Ihres Agenten ein.
 - Wählen Sie Schlüssel abrufen aus.
- Wenn die Aktivierung fehlschlägt, [überprüfen Sie Ihre Netzwerkkonfiguration](#) anhand des von Ihnen verwendeten Dienstendpunkts.
- Wählen Sie Den Aktivierungsschlüssel Ihres Agenten manuell eingeben, wenn Sie keine Verbindung zwischen Ihrem Browser und dem Agenten herstellen möchten.
 - [Rufen Sie den Schlüssel](#) von der lokalen Agentenkonsole oder mithilfe eines `curl` Befehls ab.
 - Zurück in der DataSync Konsole geben Sie den Schlüssel in das Feld Aktivierungsschlüssel ein.
5. (Empfohlen) Geben Sie Ihrem Agenten als Agentenname einen Namen, den Sie sich merken können.
6. (Optional) Geben Sie für Tags Werte für die Felder Schlüssel und Wert ein, um Ihren Agenten zu taggen.

Mithilfe von Stichwörtern können Sie Ihre AWS Ressourcen verwalten, filtern und nach ihnen suchen.

7. Wählen Sie **Create agent** (Agent erstellen) aus.
8. Stellen Sie auf der Seite **Agents** sicher, dass Ihr Agent den richtigen Service-Endpunkt-Typ verwendet.

 Note

Zu diesem Zeitpunkt stellen Sie möglicherweise fest, dass Ihr Agent offline ist. Dies geschieht kurz nach der Aktivierung eines Agenten.

AWS CLI

1. Sobald Sie [Ihren Aktivierungsschlüssel erhalten](#) haben, kopieren Sie je nach Art des verwendeten Dienstendpunkts einen der folgenden `create-agent` Befehle:

- Öffentlicher oder FIPS-Dienstendpunkt:

```
aws datasync create-agent \  
  --activation-key activation-key \  
  --agent-name name-for-agent
```

- VPC- oder FIPS-VPC-Dienstendpunkt:

```
aws datasync create-agent \  
  --activation-key activation-key \  
  --agent-name name-for-agent \  
  --vpc-endpoint-id vpc-endpoint-id \  
  --subnet-arns subnet-arn \  
  --security-group-arns security-group-arn
```

2. Geben Sie für `--activation-key` Ihren [Agenten-Aktivierungsschlüssel](#) an.
3. (Empfohlen) Geben Sie für `--agent-name` einen Namen für Ihren Agenten ein, an den Sie sich erinnern können.
4. Wenn Sie einen VPC-Dienstendpunkt verwenden, geben Sie die folgenden Optionen an:

- Geben Sie für `--vpc-endpoint-id` die ID des VPC-Dienstendpunkts an, den Sie verwenden.
 - Geben Sie für den ARN des Subnetzes an `--subnet-arns`, in dem sich Ihr VPC-Dienstendpunkt befindet.
 - Geben Sie für `--security-group-arns` den ARN der Sicherheitsgruppe an, die den für die Verwendung von DataSync [VPC-Dienstendpunkten](#) erforderlichen Datenverkehr zulässt.
5. Führen Sie den Befehl `create-agent` aus.

Sie erhalten eine Antwort mit dem ARN des Agenten, den Sie gerade aktiviert haben.
Beispiel:

```
{
  "AgentArn": "arn:aws:datasync:us-east-1:111222333444:agent/
agent-0b0addbeef44baca3"
}
```

6. Stellen Sie sicher, dass Ihr Agent aktiviert ist, indem Sie den `list-agents` folgenden Befehl ausführen:

```
aws datasync list-agents
```

 Note

Zu diesem Zeitpunkt stellen Sie möglicherweise fest, dass Ihr Agent dies Status ist `OFFLINE`. Dies geschieht kurz nach der Aktivierung eines Agenten.

DataSync API

Sobald Sie [Ihren Aktivierungsschlüssel erhalten](#) haben, aktivieren Sie Ihren Agenten mithilfe des [CreateAgent](#) Vorgangs.

 Note

Wenn Sie fertig sind, stellen Sie möglicherweise fest, dass Ihr Agent offline ist. Dies geschieht kurz nach der Aktivierung eines Agenten.

Nächste Schritte

- [Überprüfen Sie die Verbindung Ihres Agenten](#) zu Ihrem Speichersystem und dem DataSync Service.
- Wenn Sie bei der Aktivierung Ihres Agenten auf Probleme stoßen, erhalten Sie Hilfe bei der [Fehlerbehebung](#).
- Erstellen Sie den DataSync Standort, den Sie mit Ihrem Agenten verwenden möchten. Dies kann ein [lokaler](#) oder ein [anderer Cloud-Standort](#) sein.

Überprüfen Sie die Netzwerkverbindungen Ihres Agenten

Stellen Sie nach der Aktivierung Ihres AWS DataSync Agenten sicher, dass der Agent über eine Netzwerkverbindung zu Ihrem Speichersystem und dem DataSync Service verfügt.

Greifen Sie auf die lokale Konsole Ihres Agenten zu

Wie Sie auf die lokale Konsole Ihres Agenten zugreifen, hängt von der Art des Agenten ab, den Sie verwenden.

Zugreifen auf die lokale Konsole (VMware ESXi, Linux KVM oder Microsoft Hyper-V)

Aus Sicherheitsgründen können Sie keine Remoteverbindung zur lokalen Konsole der virtuellen DataSync Agentenmaschine (VM) herstellen.

- Wenn Sie die lokale Konsole zum ersten Mal verwenden, melden Sie sich mit den Standardanmeldedaten an. Der Standardbenutzername lautet **admin**, das Passwort ist **password**.

Note

Wir empfehlen das Ändern des Standard-Passworts. Geben Sie dazu im Hauptmenü der Konsole **5** (oder **6** für VMware VMs) ein und führen Sie dann den `passwd` Befehl zum Ändern des Kennworts aus.

Zugreifen auf die lokale Konsole (Amazon EC2)

Um eine Verbindung zur lokalen Konsole eines EC2 Amazon-Agenten herzustellen, müssen Sie SSH verwenden.

Bevor Sie beginnen: Stellen Sie sicher, dass die Sicherheitsgruppe Ihrer EC2 Instance den Zugriff mit SSH (TCP-Port 22) zulässt.

1. Öffnen Sie ein Terminal und kopieren Sie den folgenden ssh Befehl:

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Geben Sie für */path/key-pair-name* den Pfad und den Dateinamen (.pem) des privaten Schlüssels an, der für die Verbindung mit Ihrer Instance erforderlich ist.
 - Legen Sie für *instance-user-name* die Option admin fest.
 - Geben Sie für *instance-public-ip-address* die öffentliche IP-Adresse Ihrer Instance an.
2. Führen Sie den ssh Befehl aus, um eine Verbindung mit der Instance herzustellen.

Sobald die Verbindung hergestellt ist, wird das Hauptmenü der lokalen Konsole des Agenten angezeigt.

Überprüfen Sie die Verbindung Ihres Agenten zu Ihrem Speichersystem

Testen Sie, ob Ihr DataSync Agent eine Verbindung zu Ihrem Speichersystem herstellen kann. Weitere Informationen finden Sie unter [1. Netzwerkverbindung zwischen Ihrem Speichersystem und dem Agenten](#).

1. [Greifen Sie auf die lokale Konsole Ihres Agenten](#) zu.
2. Geben Sie im Hauptmenü AWS DataSync Aktivierung — Konfiguration die Eingabetaste ein³.
3. Geben Sie eine der folgenden Optionen ein:
 - a. Geben Sie ein¹, um eine NFS-Serververbindung zu testen.
 - b. Geben Sie ein², um eine SMB-Serververbindung zu testen.
 - c. Geben Sie ein³, um eine Object Storage-Server-Verbindung zu testen.
 - d. Geben Sie ein⁴, um eine HDFS-Verbindung zu testen.
 - e. Geben Sie ein⁵, um eine Microsoft Azure Blob Storage Verbindung zu testen.

4. Geben Sie die IP-Adresse oder den Domainnamen des Speicherservers ein.

Beachten Sie bei der Eingabe der IP-Adresse oder des Domainnamens Folgendes:

- Fügen Sie kein Protokoll hinzu. Geben Sie beispielsweise **mystorage.com** statt von **https://mystorage.com**.
 - Geben Sie für HDFS die IP-Adresse oder den Domänennamen des NameNode oder DataNode im Hadoop-Cluster ein.
5. Wenn Sie dazu aufgefordert werden, geben Sie den TCP-Port für die Verbindung zum Speicherserver ein (z. B. **443**).

Prüfen Sie, ob der Konnektivitätstest BESTANDEN oder FEHLGESCHLAGEN ist.

Überprüfen Sie die Verbindung Ihres Agenten mit dem Dienst DataSync

Testen Sie, ob Ihr DataSync Agent eine Verbindung zum DataSync Dienst herstellen kann. Weitere Informationen finden Sie unter [2. Netzwerkverbindung zwischen Ihrem Agenten und DataSync dem Service](#).

1. [Greifen Sie auf die lokale Konsole Ihres Agenten](#) zu.
2. Geben Sie im Hauptmenü AWS DataSync Aktivierung — Konfiguration die Eingabetaste ein, **2** um mit dem Testen der Netzwerkkonnektivität zu beginnen.

Wenn Ihr Agent aktiviert ist, kann die Option Netzwerkkonnektivität testen ohne zusätzliche Benutzereingabe gestartet werden, da die Region und der Endpunktyp den aktivierten Agenteninformationen entnommen werden.

3. Geben Sie den Typ des DataSync Service-Endpunkts ein, den Ihr Agent verwendet:
 - a. Geben Sie für Endpunkte des öffentlichen Dienstes ein **1** und den AWS-Region Ort, an dem Ihr Agent aktiviert ist.
 - b. Geben Sie für FIPS-Dienstendpunkte die Region ein **2**, in der Ihr Agent aktiviert ist.
 - c. Geben Sie für VPC-Dienstendpunkte ein. **3**
 - d. Geben Sie für FIPS-VPC-Dienstendpunkte den Wert ein. **4**

Sie sehen die Meldung PASSED oder FAILED.

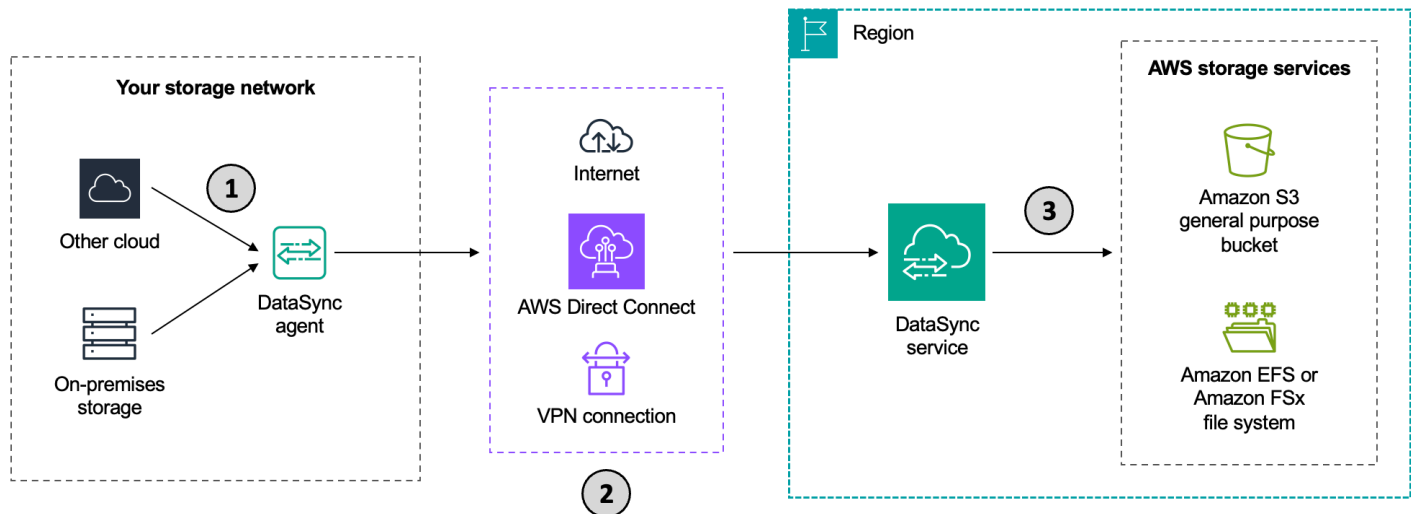
4. Wenn die Meldung FEHLGESCHLAGEN angezeigt wird, überprüfen Sie Ihre Netzwerkkonfiguration. Weitere Informationen finden Sie unter [AWS DataSync Netzwerkanforderungen](#).

Nächste Schritte

Erstellen Sie den DataSync Standort, den Sie mit Ihrem Agenten verwenden möchten. Dies kann ein [lokaler](#) oder ein [anderer Cloud-Standort](#) sein.

Ihr Netzwerk für AWS DataSync Übertragungen verbinden

Wenn [Sie einen AWS DataSync Agenten benötigen](#), müssen Sie mehrere Netzwerkverbindungen für eine Datenübertragung einrichten. Das folgende Diagramm zeigt die drei Netzwerkverbindungen bei einer DataSync Übertragung von einem Speichersystem (das sich vor Ort, in einer anderen Cloud oder am Edge befinden kann) zu einem AWS Speicherdienst.



1. Netzwerkverbindung zwischen Ihrem Speichersystem und dem Agenten

Ihr DataSync Agent stellt eine Verbindung zu Ihrem lokalen Speicher oder Speicher in anderen Clouds her. Weitere Informationen finden Sie unter [Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher](#).

2. Netzwerkverbindung zwischen Ihrem Agenten und DataSync dem Service

Bei der Verbindung Ihres Agenten mit dem DataSync Service gibt es einige Aspekte. Zunächst müssen Sie eine Netzwerkverbindung zwischen Ihrem Speicherort und herstellen AWS. Zweitens benötigt Ihr Agent einen Service-Endpunkt, mit dem er kommunizieren kann DataSync.

Inhalt

- [Verbinden Sie Ihr Speichernetzwerk mit AWS](#)

- [Auswählen eines Service-Endpunkts](#)

Verbinden Sie Ihr Speichernetzwerk mit AWS

Beachten Sie bei der Verwendung DataSync die folgenden Optionen für die Verbindung Ihres Speichernetzwerks mit AWS:

- Direct Connect- Mit [Direct Connect](#) können Sie eine dedizierte Verbindung zwischen Ihrem Speichernetzwerk und herstellen AWS. Aus einer bestimmten DataSync Perspektive können Sie auf diese Weise:
 - Übertragen Sie Daten über einen privaten Pfad in Ihre Virtual Private Cloud (VPC), wodurch das Routing über das öffentliche Internet vermieden wird.
 - Sorgen Sie für eine vorhersehbarere Verbindung als die Verwendung eines virtuellen privaten Netzwerks (VPN), um Ihr Speichernetzwerk zu verbinden AWS (insbesondere, wenn es sich bei Ihrem Agenten um eine EC2 Amazon-Instance handelt).
 - Verwenden Sie eine beliebige Art von DataSync Dienstendpunkt, einschließlich [öffentlicher Endpunkte](#), [Federal Information Processing Standard \(FIPS\)](#) oder [VPC-Endpunkte](#).

Weitere Informationen finden Sie unter [DataSync Architektur- und Routing-Beispiele mit Direct Connect](#).

- VPN — Sie können Ihr Speichernetzwerk mit AWS einem VPN (z. B.) verbinden. [AWS Site-to-Site VPN](#)
- Öffentliches Internet — Sie können Ihr Speichernetzwerk direkt mit dem DataSync Internet verbinden, indem Sie einen [öffentlichen](#) Endpunkt oder einen [FIPS-Serviceendpunkt](#) verwenden.

Auswählen eines Service-Endpunkts

Ihr Agent verwendet einen Service-Endpunkt für die Kommunikation mit DataSync. Weitere Informationen finden Sie unter [Wählen Sie einen Service-Endpunkt für Ihren Agenten AWS DataSync](#).

3. Netzwerkverbindung zwischen DataSync Dienst und AWS Speicherdienst

Um eine Verbindung DataSync zu einem AWS Speicherdienst herzustellen, müssen Sie lediglich sicherstellen, dass der DataSync Dienst auf Ihren S3-Bucket oder Ihr Dateisystem zugreifen kann. Weitere Informationen finden Sie unter [Netzwerkanforderungen für AWS Speicherdienste](#).

Netzwerkbetrieb, wenn Sie keinen DataSync Agenten benötigen

Bei Übertragungen, für die [kein DataSync Agent erforderlich](#) ist, müssen Sie lediglich sicherstellen, dass der DataSync Service auf die AWS Speichersysteme zugreifen kann, zwischen denen Sie Daten übertragen. Weitere Informationen finden Sie unter [Netzwerkanforderungen für AWS Speicherdienste](#).

Wie und wo der DataSync Verkehr durch das Netzwerk fließt

DataSync hat Verkehr auf Datenebene und Kontrollebene. Es ist wichtig zu wissen, wie die einzelnen Daten durch das Netzwerk fließen, wenn Sie Ihren DataSync Datenverkehr trennen möchten.

- **Datenverkehr auf Datenebene** — Beinhaltet die Datei- oder Objektdaten, die zwischen Ihren Speicherorten übertragen werden. In den meisten Fällen wird der Datenverkehr auf der Datenebene über [Netzwerkschnittstellen](#) geleitet, die DataSync automatisch generiert und verwaltet werden, wenn Sie eine Aufgabe erstellen. Wo diese Netzwerkschnittstellen erstellt werden, hängt von der Art des AWS Speicherdienstes ab, zu dem oder von dem Sie Daten übertragen, und vom Dienstendpunkt, den Ihr DataSync Agent verwendet.
- **Steuern Sie den Flugverkehr** — Beinhaltet Verwaltungsaktivitäten für Ihre DataSync Ressourcen. Dieser Datenverkehr wird über den Service-Endpunkt geleitet, den Ihr Agent verwendet.

Netzwerksicherheit für DataSync

Informationen darüber, wie Ihre Speicherdaten (einschließlich Metadaten) während einer Übertragung gesichert werden, finden Sie unter [AWS DataSync Verschlüsselung bei der Übertragung](#).

AWS DataSync Netzwerkanforderungen

Die Konfiguration Ihres Netzwerks ist ein wichtiger Schritt bei der Einrichtung AWS DataSync. Ihre Netzwerkkonfiguration hängt von mehreren Faktoren ab, z. B. von der Art der Speichersysteme, mit denen Sie arbeiten. Es hängt auch davon ab, welche Art von DataSync Service-Endpunkt Sie verwenden möchten.

IPv6 Unterstützung

DataSync bietet Dual-Stack-Unterstützung für Kompatibilität mit IPv4 IPv6 Netzwerken. IPv6 Support ist überall verfügbar AWS-Regionen , wo der Service angeboten wird. DataSync unterstützt die Verwendung von IPv6 Adressen mit den folgenden Datenquellen:

- Elastisches Dateisystem (EFS)
- Network File System (NFS)
- Server-Nachrichtenblock (SMB)
- Objektspeicher

IPv6-kompatible Agenten für lokalen Speicher

Für die Verwendung DataSync in einer IPv6 Netzwerkumgebung müssen Sie IPv6 -kompatible Agenten verwenden. Diese Agenten unterstützen sowohl Konnektivität als auch IPv6 Konnektivität IPv4 und passen sich an verschiedene Netzwerkumgebungen an.

- IPv6Nur für Netzwerke — keine Konfigurationsänderungen erforderlich.
- Für IPv4 reine Netzwerke — keine Konfigurationsänderungen erforderlich.
- Bei Dual-Stack-Netzwerken (IPv4 sowohl als auch IPv6) — lassen Sie den Agenten das Protokoll auswählen oder konfigurieren Sie es manuell nach Ihren Wünschen.

Überlegungen zu Dual-Stack-Netzwerken

Sie können das Verhalten Ihres Agenten über die lokale Konsole auf folgende Weise anpassen:

- Deaktivieren Sie diese Option, IPv6 damit der Agent nicht IPv6 auf lokale Dateisysteme oder den DataSync Dienst zugreifen kann.
- Stellen Sie die IP-Version des Agenten ein, die für Datenübertragungen verwendet werden soll:

- Stellen Sie diese IPv6 Option so ein, dass der Agent sie nur IPv6 für Datenübertragungen verwendet.
- Stellen Sie diese Option IPv4 so ein, dass der Agent sie nur IPv4 für Datenübertragungen verwendet.
- Auf Auto setzen (stellt die Standardeinstellung wieder her), sodass der Agent automatisch die Protokollversion (IPv4 oder IPv6) für Datenübertragungen auswählt.

Weitere Informationen zur Verwaltung der IP-Versionseinstellungen für Agenten finden Sie unter [the section called “Durchführung von Wartungsarbeiten an Ihrem Agenten”](#).

 Important

Agenten, die aus Images erstellt wurden, die vor dem 16. Juli 2025 heruntergeladen wurden, bieten keine Unterstützung IPv6.

Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher

Die folgenden Netzwerkanforderungen können für lokale, selbstverwaltete und andere Cloud-Speichersysteme gelten. In der Regel handelt es sich dabei um Speichersysteme, die Sie verwalten oder die möglicherweise von einem anderen Cloud-Anbieter verwaltet werden.

 Note

Abhängig von Ihrem Netzwerk müssen Sie möglicherweise Datenverkehr an anderen als den hier aufgeführten Ports zulassen, damit Ihr DataSync Agent eine Verbindung zu Ihrem Speicher herstellen kann.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet von DataSync
DataSync Agent	NFS-Dateiserver	TCP	2049 (für die NFS- Versionen	Hängt den NFS-Datei server ein.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet von DataSync
			4.1 und 4.0) 111 und 2049 (für NFS-Versi on 3.x)	DataSync unterstützt die NFS-Versionen 3.x, 4.0 und 4.1.
DataSync Agent	SMB-Dateiserver	TCP	139 oder 445	Hängt den SMB-Datei server ein. DataSync unterstützt SMB-Versionen 1.0 und höher. Aus Sicherhei tsgründen empfehlen wir die Verwendung von SMB Version 3.0.2 oder höher. Frühere Versionen , wie SMB 1.0, enthalten bekannte Sicherhei tslücken, die Angreifer ausnutzen können, um Ihre Daten zu gefährden.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet von DataSync
DataSync Agent	Objektspeicher	TCP	443 (HTTPS) oder 80 (HTTP)	Greift auf Ihren Amazon S3-kompatiblen Objektspeicher vor Ort oder in anderen Clouds zu.

 Note

Abhängig von Ihrem Objektspeicher müssen Sie möglicherweise Datenverkehr an nicht standardmäßigen HTTPS und HTTP-Ports (z. B. 8443 oder 8080) zulassen.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet von DataSync
DataSync Agent	Hadoop-Cluster	TCP	NameNode Port (Standard ist 8020) In den meisten Clustern finden Sie diese Portnumme r in der core- site .xml Datei unter der fs.default.name Eigenscha ft fs.default oder (abhängig von der Hadoop-Di stribution).	Greift auf den NameNodes in Ihrem Hadoop-Cluster zu. Geben Sie den Port an, der beim Erstellen eines HDFS-Speicherorts verwendet wird.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet von DataSync
DataSync Agent	Hadoop-Cluster	TCP	DataNode Port (Standard ist 50010) In den meisten Clustern finden Sie diese Portnumme r in der hdfs- site .xml Datei unter der dfs.datan ode.addre ss Eigenscha ft.	Greift auf den DataNodes in Ihrem Hadoop-Cluster zu. Der DataSync Agent bestimmt automatisch den zu verwendenden Port.
DataSync Agent	Hadoop-Schlüsselve rwaltungsserver (KMS)	TCP	KMS-Port (Standard ist 9600)	Greift auf den KMS für Ihren Hadoop-Cluster zu.
DataSync Agent	Kerberos Key Distribution Center (KDC) -Server	TCP	KDC-Port (Standard ist 88)	Authentifiziert sich mit dem Kerberos-Bereich. Dieser Port wird nur für HDFS- und SMB- Standorte verwendet, die die Kerberos-Authentif izierung verwenden.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet von DataSync
DataSync Agent	Verwaltungsschnittstelle des Speichersystems	TCP	Hängt von Ihrem Netzwerk ab	Stellt eine Verbindung zu Ihrem Speichersystem her.

Netzwerkanforderungen für AWS Speicherdienste

Die Netzwerkanschlüsse DataSync, die für die Verbindung mit einem AWS Speicherdienst während einer Übertragung erforderlich sind, variieren.

Aus	Bis	Protocol (Protokoll)	Port
DataSync Dienst	Amazon EFS	TCP	2049
DataSync Dienst	FSx für Windows-Dateiserver	Weitere Informationen finden Sie unter Dateisystem-Zugriffskontrolle FSx für Windows-Dateiserver .	
DataSync Dienst	FSx für Lustre	Weitere Informationen finden Sie unter Dateisystem-Zugriffskontrolle FSx für Lustre .	
DataSync Dienst	FSx für OpenZFS	Siehe Dateisystem-Zugriffskontrolle FSx für OpenZFS .	
DataSync Dienst	FSx für ONTAP	TCP	111, 635 und 2049 (NFS) 445 (SMB)
DataSync Bedienung	Amazon S3	N/A (DataSync stellt in Ihrem Namen eine Verbindung zu S3-Buckets her)	

Netzwerkanforderungen für öffentliche Endpunkte oder FIPS-Dienstendpunkte

Ihr DataSync Agent benötigt den folgenden Netzwerkzugriff, wenn er öffentliche Endpunkte oder FIPS-Dienstendpunkte verwendet. Wenn Sie eine Firewall oder einen Router verwenden, um den Netzwerkverkehr zu filtern oder einzuschränken, konfigurieren Sie Ihre Firewall oder Ihren Router so, dass diese Endpunkte zugelassen werden.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
Ihr Webbrowser	DataSync Agent	TCP	80 (HTTP)	Ermöglicht Ihrem Browser, den Aktivierungsschlüssel des DataSync Agenten abzurufen. . DataSync Schließt nach der Aktivierung den Port 80 des Agenten. Ihr Agent benötigt nicht, dass Port 80 öffentlich zugänglich ist. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkonfiguration ab.	–

Aus	Bis	Protocol (Protokol I)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
				 Note Sie können den Aktivierungsschlüssel erhalten, ohne dass eine Verbindung zwischen Ihrem Browser und dem Agenten hergestellt werden muss. Weitere Informationen finden Sie unter Einen Aktivierungsschlüssel	

Aus	Bis	Protocol (Protokol I)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
				sel erhalten.	
DataSync Agent	Amazon CloudFront	TCP	443 (HTTPS)	Hilft Ihrem DataSync Agenten vor der Aktivierung beim Bootstrap ping. Nur für Agenten im Basismodus erforderlich.	AWS-Regionen: - d3dvvaliwoko8h.cloudfront.net AWS GovCloud (US) Regionen: - s3.us-gov-west-1.amazonaws.com/fmrse-ndpoints-endpoints-bucket-go4p5gpna6sk
DataSync Agent	AWS	TCP	443 (HTTPS)	Aktiviert Ihren DataSync Agenten und ordnet ihn Ihrem zu AWS- Konto. Sie können den öffentlichen Endpunkt nach der Aktivierung blockieren.	AWS-Region Dort aktivieren Sie Ihren DataSync Agenten. <i>activation-region</i> Aktivierung öffentlicher Endgeräte: - activation.datasyn c. <i>activation- region</i>.amazonaws.com Aktivierung von FIPS-Endpunkten: - activation.datasyn c-fips. <i>activation- region</i>.amazonaws.com

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
DataSync Agent	AWS	TCP	443 (HTTPS)	Ermöglicht die Kommunikation zwischen dem DataSync Agenten und dem DataSync Service-Endpoint. Weitere Informationen finden Sie unter Wählen Sie einen Service-Endpoint für Ihren Agenten AWS DataSync.	AWS-Region Hier aktivieren Sie Ihren DataSync Agenten. <i>activation-region</i> Je nachdem, wofür Sie es verwenden DataSync , müssen Sie möglicherweise nicht allen hier aufgeführten Endpunkten Zugriff gewähren. DataSync Endpunkte der Steuerungsebene: • Öffentlicher Endpunkt: <code>cp.datasync. <i>activation-region</i> .amazonaws.com</code> • FIPS-Endpunkt: <code>cp.datasync-fips. <i>activation-region</i> .amazonaws.com</code> DataSync Endpunkt der Datenebene (nur für Übertragungsaufgaben): • Agenten im Basismodus: <code><i>your-task-id</i> .datasync-dp. <i>activation-region</i> .amazonaws.com</code> Agenten im erweiterten Modus: <code>*.*.<i>your-task-id</i> .*. <i>activation-region</i> .amazonaws.com</code>

Aus	Bis	Protocol (Protokol I)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
Ihr Kunde	AWS	TCP	443 (HTTPS)	Ermöglicht es Ihnen, DataSync API-Anfragen zu stellen.	AWS-Region Dort aktivieren Sie Ihren DataSync Agenten. <i>activation-region</i> Öffentlicher Endpunkt: • <code>datasync.<i>activation-region</i>.amazonaws.com</code> FIPS-Endpunkt: • <code>datasync-fips.<i>activation-region</i>.amazonaws.com</code>

Aus	Bis	Protocol (Protokol I)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
DataSync Agent	AWS	TCP	443 (HTTPS)	Ermöglicht dem DataSync Agenten, Updates von zu erhalten AWS. Weitere Informationen finden Sie unter Ihren AWS DataSync Agenten verwalten .	AWS-Region Dort aktivieren Sie Ihren DataSync Agenten. <i>activation-region</i> Agenten im Basismodus: - amazonlinux.default.amazonaws.com - cdn.amazonlinux.com - amazonlinux-2-repos-<i>activation-region</i>.s3.dualstack.<i>activation-region</i>.amazonaws.com - amazonlinux-2-repos-<i>activation-region</i>.s3.<i>activation-region</i>.amazonaws.com *.s3.<i>activation-region</i>.amazonaws.com *.s3.dualstack.<i>activation-region</i>.amazonaws.com Agenten im erweiterten Modus: *.s3.dualstack.<i>activation-region</i>.amazonaws.com

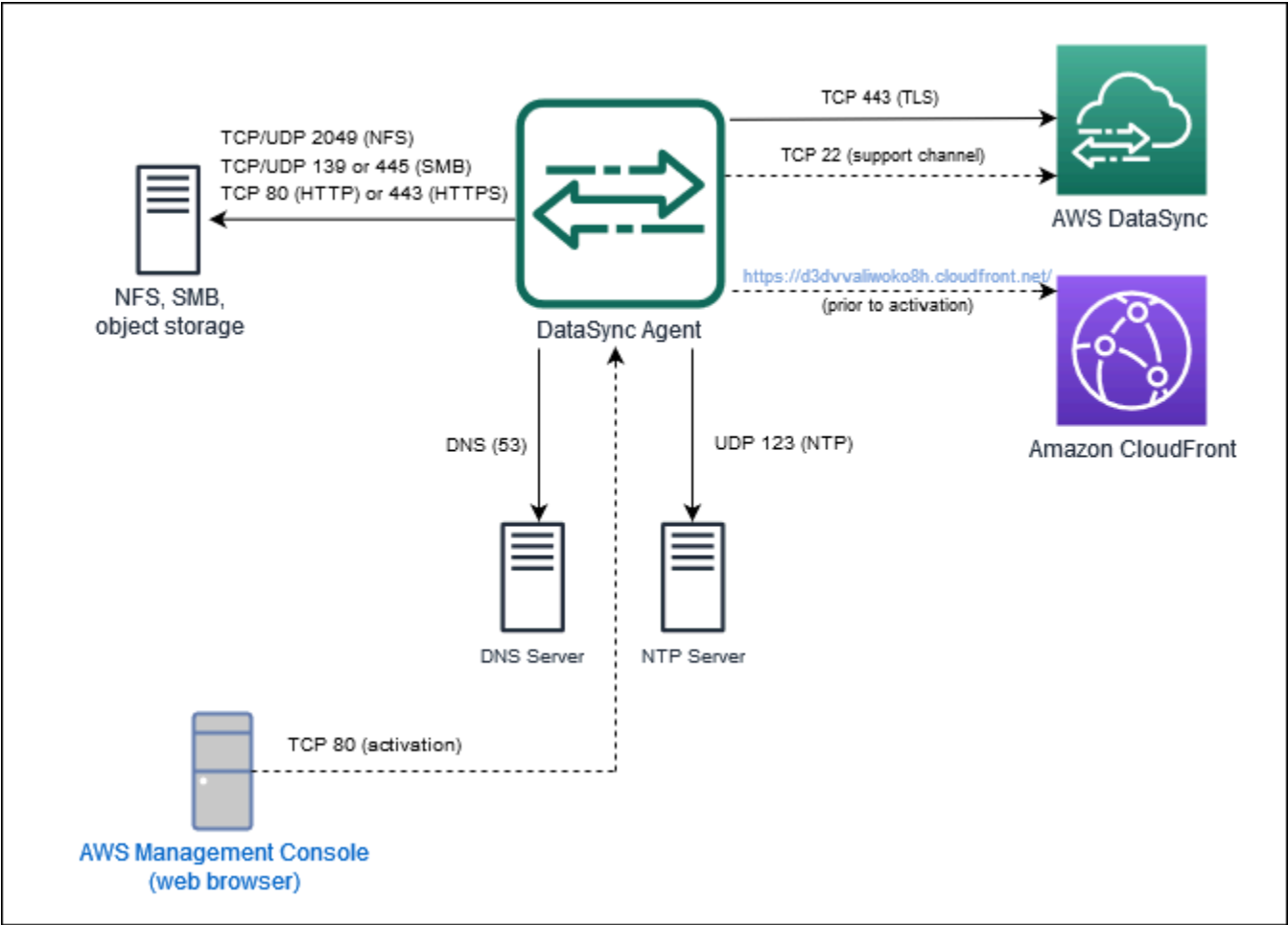
Aus	Bis	Protocol (Protokol I)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
DataSync Agent	Domain Name Service (DNS)- Server	TCP/ UDP	53 (DNS)	Ermöglicht die Kommunika tion zwischen dem DataSync Agenten und dem DNS- Server.	–
DataSync Agent	AWS	TCP	22 (Support- Kanal)	Ermöglicht AWS Support den Zugriff auf Ihren DataSync Agenten, der Ihnen bei der Behebung von Problemen hilft. Dieser Port muss für den normalen Betrieb nicht geöffnet sein.	Agenten im Basismodus: - Gewerbliche Regionen: 54.201.223.107 - GovCloud Regionen: 52.222.99.142 Agenten im erweiterten Modus: - Gewerbliche Regionen: support.datasync.us- east-1.amazonaws.com - GovCloud Regionen: support.datasync.u s-gov-west-1.amazo naws.com

Aus	Bis	Protocol (Protokol I)	Port	Wie wird es verwendet	Endpunkte, auf die zugegriffen wurde
DataSync Agent	Network Time Protocol (NTP)- Server	UDP	123 (NTP)	Ermöglicht lokalen Systemen, die VM-Zeit mit der Host-Zeit zu synchronisieren.	NTP: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org

 **Note**

Informationen zum Ändern der Standard-NTP-Konfiguration Ihres VM-Agenten zur Verwendung eines anderen NTP-Servers mithilfe der lokalen Konsole finden Sie unter. [Serverkonfiguration für die Systemzeit des Agenten anzeigen und verwalten](#)

Das folgende Diagramm zeigt die Ports, die für die DataSync Verwendung von öffentlichen oder FIPS-Dienstendpunkten erforderlich sind.



Netzwerkanforderungen für VPC- oder FIPS-VPC-Dienstendpunkte

Ein VPC-Endpunkt (Virtual Private Cloud) bietet eine private Verbindung zwischen Ihrem Agenten AWS , die weder das Internet überquert noch öffentliche IP-Adressen verwendet. Dadurch wird auch verhindert, dass Pakete in das Netzwerk gelangen oder es verlassen. Weitere Informationen finden Sie unter [Auswahl eines VPC-Serviceendpunkts](#).

DataSync benötigt die folgenden Ports, damit Ihr Agent einen VPC-Dienstendpunkt verwenden kann.

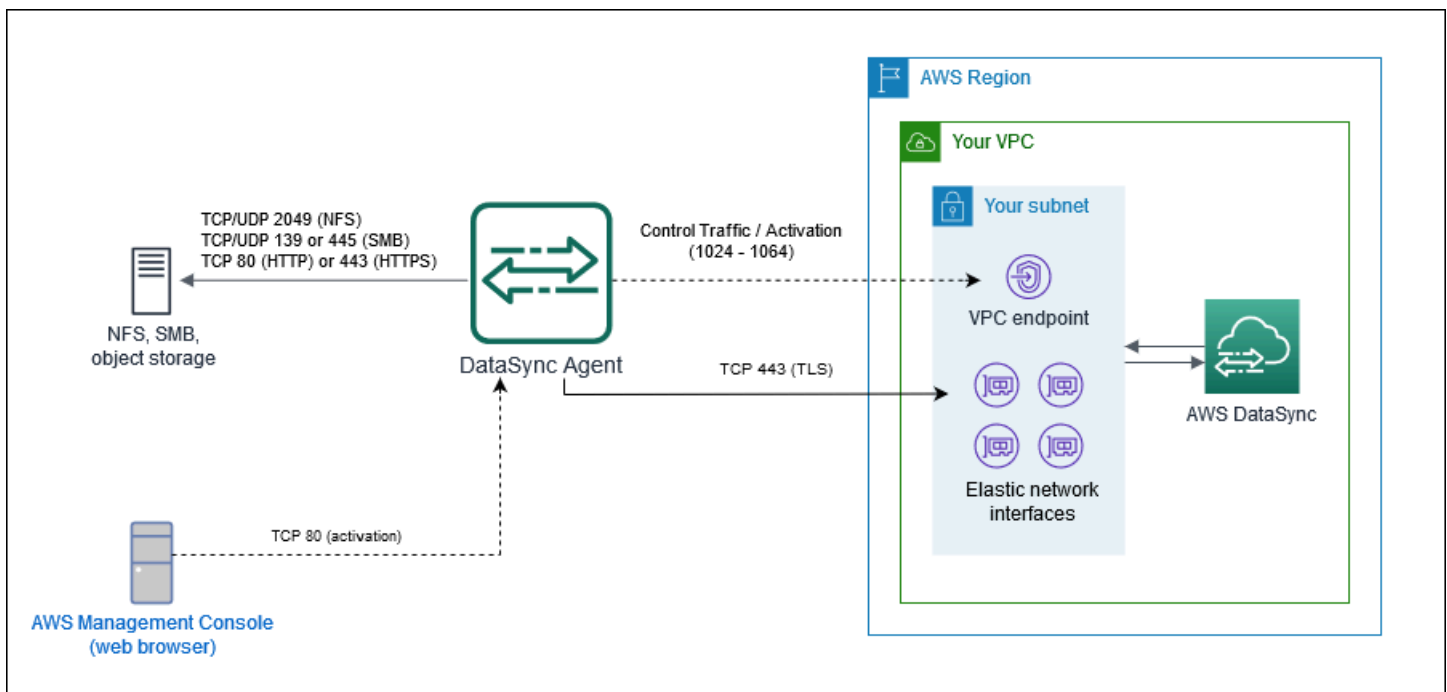
Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet
Ihr Webbrowser	Ihr DataSync Agent	TCP	80 (HTTP)	Ermöglicht Ihrem Browser, den Agenten-Aktivierungsschlüssel abzurufen. DataSync

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet
				Schließt nach der Aktivierung den Port 80 des Agenten. Ihr Agent benötigt nicht, dass Port 80 öffentlich zugänglich ist. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkonfiguration ab.  Note Sie können den Aktivierungsschlüssel erhalten, ohne dass eine Verbindung zwischen Ihrem Browser und dem Agenten hergestellt werden muss. Weitere Informationen finden Sie unter Einen Aktivierungsschlüssel erhalten.

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet
DataSync Agent	Ihr DataSync VPC-Serve-Endpunkt Um die IP-Adresse des Endpunkts zu ermitteln, öffnen Sie die Amazon VPC-Konsole, wählen Sie Endpoints und dann Ihren DataSync VPC-Service-Endpunkt aus. Suchen Sie auf der Registerkarte Subnetze die IP-Adresse für das Subnetz Ihres VPC-Dienstendpunkts. Dies ist die IP-Adresse des Endpunkts.	TCP	1024-1064	Für den Verkehr mit Kontrollflugzeugen .
DataSync Agent	Die Netzwerkschnittstellen Ihrer DataSync Aufgabe Informationen zu den IP-Adressen dieser Schnittstellen finden Sie unter Ihre Netzwerkschnittstellen anzeigen.	TCP	443 (HTTPS)	Für den Verkehr auf der Datenebene .

Aus	Bis	Protocol (Protokoll)	Port	Wie wird es verwendet
DataSync Agent	Ihr DataSync VPC-Serveeendpunkt	TCP	22 (Support-Kanal)	Um den Zugriff AWS Support auf Ihren DataSync Agenten zur Fehlerbehebung zu ermöglichen. Nur für Agenten im Basismodus erforderlich. Dieser Port muss für den normalen Betrieb nicht geöffnet sein.

Das folgende Diagramm zeigt die Ports, die für die DataSync Verwendung von VPC-Dienstendpunkten erforderlich sind.



Netzwerkschnittstellen für Übertragungen AWS DataSync

Generiert und verwaltet für jede Aufgabe, die Sie erstellen, AWS DataSync automatisch [Netzwerkschnittstellen](#) für den Datenübertragungsverkehr. Wie viele Netzwerkschnittstellen DataSync erstellt werden und wo sie erstellt werden, hängt von den folgenden Details zu Ihrer Übertragungsaufgabe ab:

- Ob für Ihre Aufgabe [ein DataSync Agent erforderlich ist](#).
- Ihre Quell- und Zielorte (von und zu denen Sie Daten kopieren).
- Der Typ des Service-Endpunkts, den Ihr Agent verwendet.

Jede Netzwerkschnittstelle verwendet eine einzelne IP-Adresse in Ihrem Subnetz (je mehr Netzwerkschnittstellen vorhanden sind, desto mehr IP-Adressen benötigen Sie). Verwenden Sie die folgenden Tabellen, um sicherzustellen, dass Ihr Subnetz über genügend IP-Adressen für Ihre Aufgabe verfügt.

Netzwerkschnittstellen für Übertragungen mit Agenten

Im Allgemeinen benötigen Sie einen DataSync Agenten, wenn Sie Daten zwischen einem AWS Speicherdienst und einem Speichersystem kopieren, bei dem dies nicht der Fall ist AWS.

Speicherort	Standardmäßig erstellte Netzwerkschnittstellen	Wo Netzwerkschnittstellen erstellt werden, wenn ein öffentlicher Endpunkt oder ein FIPS-Endpunkt verwendet wird	Wo Netzwerkschnittstellen erstellt werden, wenn ein privater (VPC) Endpunkt verwendet wird
Amazon S3	4	N/A ¹	Das Subnetz, das Sie bei der Aktivierung Ihres DataSync Agenten angeben.
Amazon EFS	4	Das Subnetz, das Sie bei der Erstellung des Amazon EFS-Standorts angeben.	

Speicherort	Standardmäßig erstellte Netzwerkschnittstellen	Wo Netzwerkschnittstellen erstellt werden, wenn ein öffentlicher Endpunkt oder ein FIPS-Endpunkt verwendet wird	Wo Netzwerkschnittstellen erstellt werden, wenn ein privater (VPC) Endpunkt verwendet wird
Amazon FSx für Windows-Dateiserver	4	Das gleiche Subnetz wie der bevorzugte Dateiserver des Dateisystems.	
Amazon FSx für Lustre	4	Das gleiche Subnetz wie das Dateisystem.	
Amazon FSx für OpenZFS	4	Das gleiche Subnetz wie das Dateisystem.	
Amazon FSx für NetApp ONTAP	4	Das gleiche Subnetz wie das Dateisystem.	

¹ Netzwerkschnittstellen werden nicht benötigt, da der DataSync Dienst direkt mit dem S3-Bucket kommuniziert.

Netzwerkschnittstellen für Übertragungen ohne Agenten

Sie benötigen keinen DataSync Agenten, wenn Sie Daten zwischen Daten kopieren AWS-Services.

Die Gesamtzahl der Netzwerkschnittstellen hängt von den DataSync Standorten Ihrer Übertragung ab. Für die Übertragung zwischen Amazon EFS- und FSx Lustre-Dateisystemen sind beispielsweise vier Netzwerkschnittstellen erforderlich. In der Zwischenzeit erfordert FSx die Übertragung zwischen einem Windows-Dateiserver und einem S3-Bucket zwei Netzwerkschnittstellen.

Speicherort	Standardmäßig erstellte Netzwerkschnittstellen	Wo Netzwerkschnittstellen erstellt werden
Amazon S3	N/A 1	N/A 1

Speicherort	Standardmäßig erstellte Netzwerkschnittstellen	Wo Netzwerkschnittstellen erstellt werden
Amazon EFS	2	Das Subnetz, das Sie bei der Erstellung des Amazon EFS-Standorts angeben.
FSx für Windows-Dateiserver	2	Das gleiche Subnetz wie der bevorzugte Dateiserver für das Dateisystem.
FSx für Lustre	2	Das gleiche Subnetz wie das Dateisystem.
FSx für OpenZFS	2	Das gleiche Subnetz wie das Dateisystem.
FSx für ONTAP	2	Das gleiche Subnetz wie das Dateisystem.

¹ Netzwerkschnittstellen werden nicht benötigt, da der DataSync Dienst direkt mit dem S3-Bucket kommuniziert.

Ihre Netzwerkschnittstellen anzeigen

Gehen Sie wie folgt vor, um die Netzwerkschnittstellen zu sehen, die Ihrer DataSync Übertragungsaufgabe zugewiesen sind:

- Verwenden Sie die [DescribeTask](#) Operation. Die Operation kehrt zurück, `SourceNetworkInterfaceArns` und `DestinationNetworkInterfaceArns` zwar mit Antworten, die wie folgt aussehen:

```
arn:aws:ec2:your-region:your-account-id:network-interface/eni-f012345678abcdef0
```

In diesem Beispiel lautet die Netzwerkschnittstellen-ID `eni-f012345678abcdef0`.

- Suchen Sie in der EC2 Amazon-Konsole nach Ihrer Aufgaben-ID (z. B. `task-f012345678abcdef0`), um deren Netzwerkschnittstellen zu finden.

DataSync Architektur- und Routing-Beispiele mit Direct Connect

Beachten Sie bei der Verwendung [Direct Connect](#) Ihrer Übertragungen die folgenden Netzwerkarchitekturen. AWS DataSync

Tip

Wenn Ihr Netzwerk ein Transit-Gateway verwendet, empfehlen wir, den logischen Pfad Ihrer DataSync Übertragung zu trennen, um die Kosten zu optimieren (insbesondere, wenn Sie eine große Datenmenge migrieren).

Wenn Sie beispielsweise den normalen Verkehr zwischen Ihren lokalen Netzwerken und virtuellen privaten Clouds (VPCs) verwenden [AWS Transit Gateway](#), können Sie Ihr Netzwerk so konfigurieren, dass der DataSync Datenverkehr das Transit-Gateway und dessen Datenverarbeitungsgebühren umgeht.

Verwenden von Direct Connect mit einem DataSync VPC-Serviceendpunkt

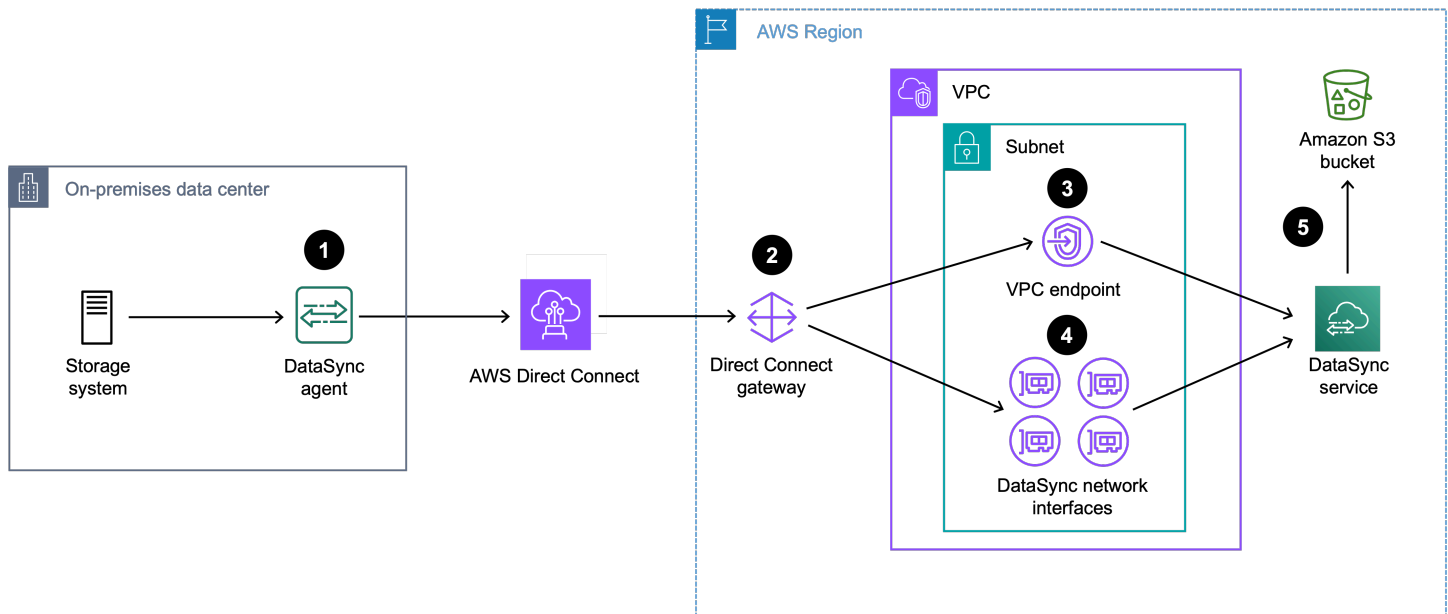
Wenn Ihr DataSync Agent einen [VPC-Serviceendpunkt](#) verwendet, benötigen Sie ein [Direct Connect-Gateway](#), um eine Verbindung zu Ihrer VPC herzustellen.

Inhalt

- [Direct Connect-Architektur mit VPC-Endpunkt und S3-Ziel](#)
- [Direct Connect-Architektur mit VPC-Endpunkt und Dateisystemziel im selben Subnetz](#)
- [Direct Connect-Architektur mit VPC-Endpunkt und Dateisystemziel in verschiedenen Subnetzen](#)

Direct Connect-Architektur mit VPC-Endpunkt und S3-Ziel

Die folgende Direct Connect-Architektur zeigt eine DataSync Übertragung von einem lokalen Speichersystem zu einem S3-Bucket.

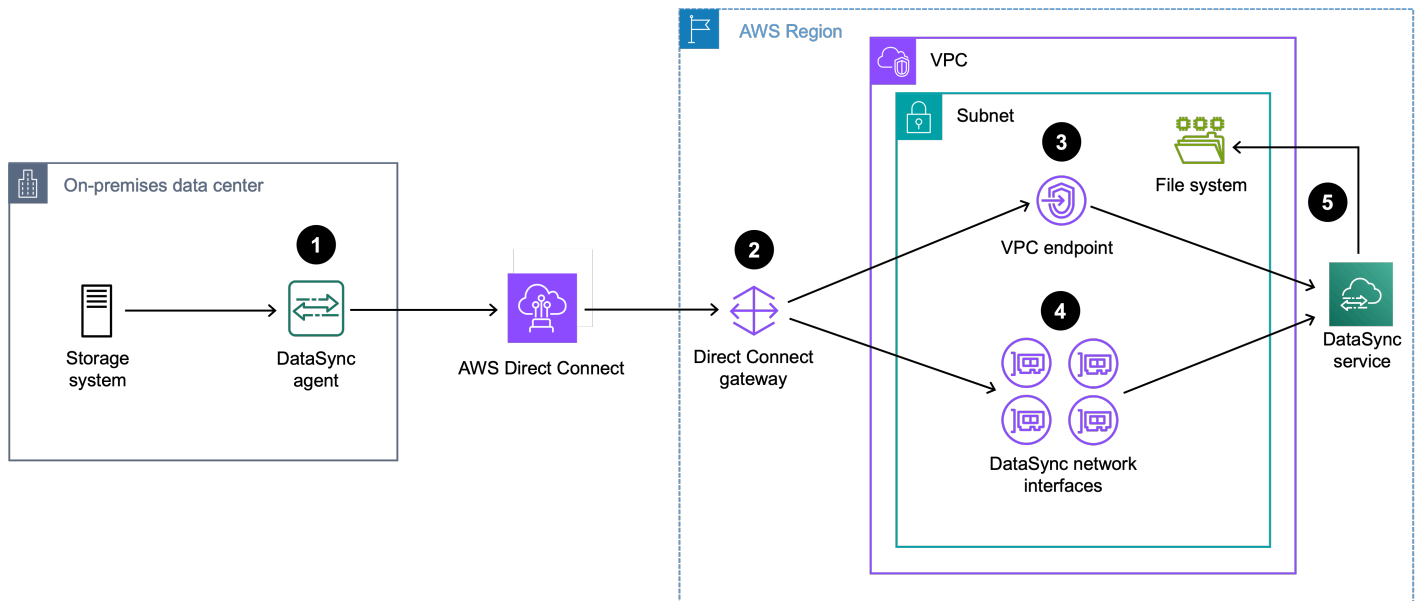


1. Der DataSync Agent leitet den DataSync Datenverkehr vom lokalen Speichersystem (Quellstandort) zur Direct Connect-Verbindung weiter.
2. DataSync Verkehrswege zu einem Direct Connect-Gateway, das für Ihre Übertragung verwendet wird. Um dies einzurichten, müssen Sie:
 - a. Ordnen Sie das Direct Connect-Gateway einem [virtuellen privaten Gateway](#) für die VPC zu. Dies ist die VPC, in der sich der DataSync VPC-Endpunkt befindet und in der die DataSync Aufgabe [Netzwerkschnittstellen](#) erstellt.
 - b. Erstellen Sie eine [private virtuelle Schnittstelle](#), die diese VPC mit dem Direct Connect-Gateway verbindet.
3. DataSync Verkehrsrouten (Kontrollebene) durch den DataSync VPC-Endpunkt.
4. DataSync Der Verkehr (Datenebene) wird durch die DataSync Netzwerkschnittstellen im Subnetz geleitet, das Sie bei der [Erstellung des DataSync](#) Agenten angegeben haben.
5. DataSync Der Verkehr leitet durch den DataSync Dienst zum S3-Bucket (Zielort).

Direct Connect-Architektur mit VPC-Endpunkt und Dateisystemziel im selben Subnetz

Bei der Übertragung zu oder von einem Amazon EFS- oder FSx Amazon-Dateisystem können sich Ihr Dateisystem und Ihr DataSync VPC-Endpunkt im selben Subnetz befinden.

Die folgende Direct Connect-Architektur zeigt eine DataSync Übertragung von einem lokalen Speichersystem zu einem Amazon EFS- oder FSx Amazon-Dateisystem.

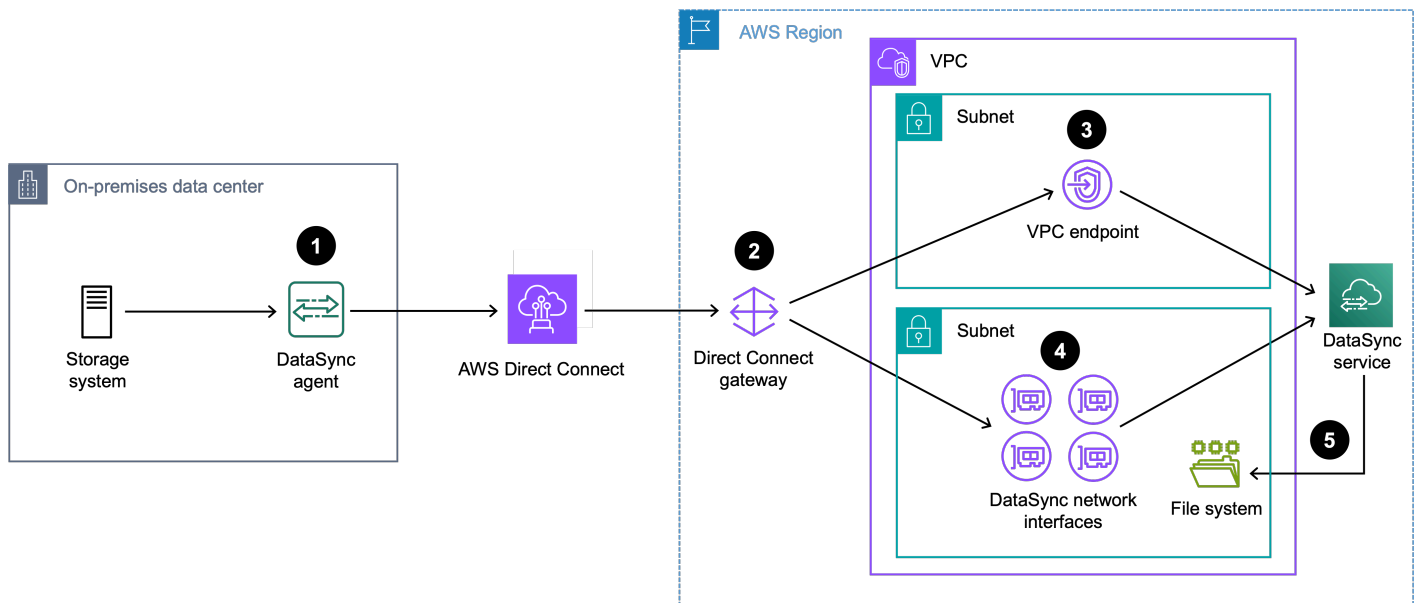


1. Der DataSync Agent leitet den DataSync Datenverkehr vom lokalen Speichersystem (Quellstandort) zur Direct Connect-Verbindung weiter.
2. DataSync Verkehrswege zu einem Direct Connect-Gateway, das für Ihre Übertragung verwendet wird. Um dies einzurichten, müssen Sie:
 - a. Ordnen Sie das Direct Connect-Gateway einem [virtuellen privaten Gateway](#) für die VPC zu. Dies ist die VPC, in der sich der DataSync VPC-Endpoint befindet und in der die DataSync Aufgabe [Netzwerkschnittstellen](#) für das Dateisystem erstellt (Zielort).
 - b. Erstellen Sie eine [private virtuelle Schnittstelle](#), die diese VPC mit dem Direct Connect-Gateway verbindet.
3. DataSync Verkehrsrouten (Kontrollebene) durch den DataSync VPC-Endpoint.
4. DataSync Der Verkehr (Datenebene) wird durch die DataSync Netzwerkschnittstellen im Subnetz des Dateisystems geleitet. Dies ist dasselbe Subnetz, in dem sich der DataSync VPC-Endpoint befindet.
5. DataSync Der Verkehr leitet durch den DataSync Dienst zum Dateisystem (Zielort).

Direct Connect-Architektur mit VPC-Endpoint und Dateisystemziel in verschiedenen Subnetzen

Bei der Übertragung zu oder von einem Amazon EFS- oder FSx Amazon-Dateisystem können sich Ihr Dateisystem und Ihr DataSync VPC-Endpoint in unterschiedlichen Subnetzen befinden.

Die folgende Direct Connect-Architektur zeigt eine DataSync Übertragung von einem lokalen Speichersystem zu einem Amazon EFS- oder FSx Amazon-Dateisystem.



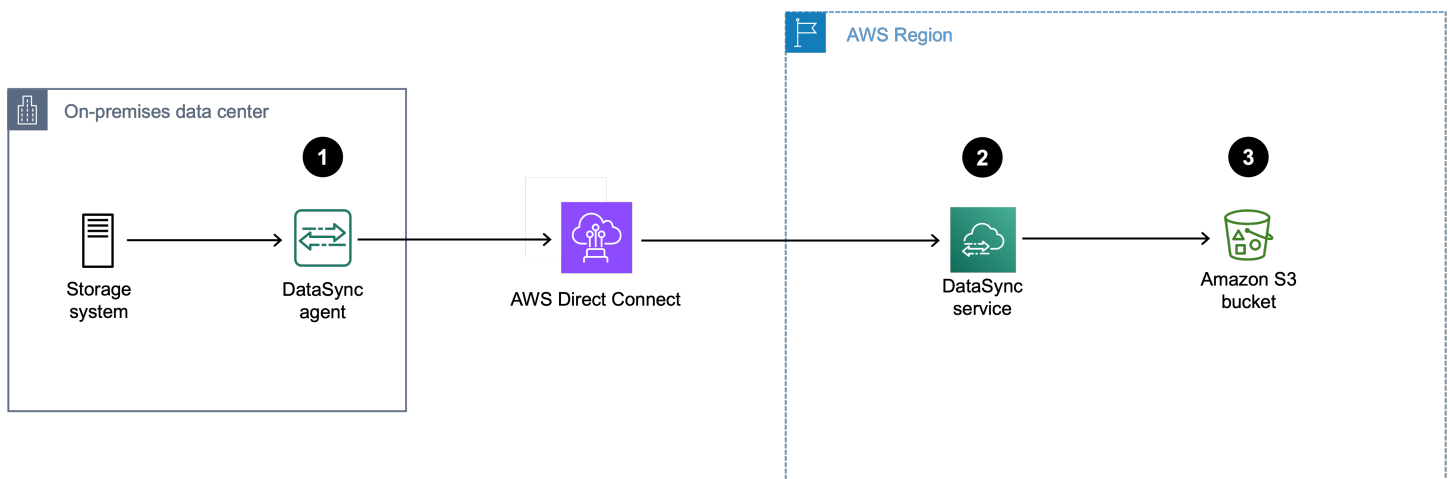
1. Der DataSync Agent leitet den DataSync Datenverkehr vom lokalen Speichersystem (Quellstandort) zur Direct Connect-Verbindung weiter.
2. DataSync Verkehrswege zu einem Direct Connect-Gateway, das für Ihre Übertragung verwendet wird. Um dies einzurichten, müssen Sie:
 - a. Ordnen Sie das Direct Connect-Gateway einem [virtuellen privaten Gateway](#) für die VPC zu. Dies ist die VPC, in der sich der DataSync VPC-Endpoint befindet und in der die DataSync Aufgabe [Netzwerkschnittstellen](#) für das Dateisystem erstellt (Zielort).
 - b. Erstellen Sie eine [private virtuelle Schnittstelle](#), die diese mit VPCs dem Direct Connect-Gateway verbindet.
3. DataSync Verkehrsrouten (Kontrollebene) durch den DataSync VPC-Endpoint.
4. DataSync Der Verkehr (Datenebene) wird durch die DataSync Netzwerkschnittstellen im Subnetz des Dateisystems geleitet. Dies ist ein anderes Subnetz als das, in dem sich der DataSync VPC-Endpoint befindet.
5. DataSync Der Verkehr leitet durch den DataSync Dienst zum Dateisystem (Zielort).

Verwenden von Direct Connect mit einem DataSync öffentlichen oder FIPS-Serviceendpunkt

Wenn Ihr DataSync Agent einen [öffentlichen](#) oder [FIPS-Dienstendpunkt \(Federal Information Processing Standard\)](#) verwendet, können Sie Ihren Datenübertragungsverkehr mithilfe einer [öffentlichen virtuellen Schnittstelle](#) über eine Direct Connect-Verbindung weiterleiten.

Direct Connect kündigt zwar standardmäßig alle lokalen und AWS-Region Remote-Präfixe an, Sie können jedoch [BGP-Community-Tags](#) verwenden, um den Umfang (regional oder global) und die Routenpräferenz des Datenverkehrs auf der öffentlichen virtuellen Schnittstelle zu steuern. Sie müssen mindestens ein öffentliches Präfix angeben, um Ihren Agenten zu erstellen. DataSync

Die folgende Direct Connect-Architektur zeigt eine DataSync Übertragung von einem lokalen Speichersystem über einen öffentlichen oder FIPS-Endpunkt zu einem S3-Bucket.



1. Der DataSync Agent leitet den DataSync Datenverkehr vom lokalen Speichersystem (Quellstandort) zur Direct Connect-Verbindung weiter.
2. DataSync Datenverkehrswege zum DataSync Dienst über eine öffentliche virtuelle Schnittstelle.
3. DataSync Verkehr zum S3-Bucket (Zielort).

Nächste Schritte

Wenn [Sie einen DataSync Agenten benötigen](#) und noch keinen erstellt haben, [stellen](#) Sie den Agenten bereit, [wählen Sie einen Service-Endpunkt](#) für den Agenten aus und [aktivieren Sie](#) dann den Agenten.

Sobald Sie den Agenten erstellt haben, können Sie [Ihr Netzwerk für konfigurieren](#) DataSync.

Konfigurieren Sie Ihren AWS DataSync Agenten für mehrere NICs

Wenn Sie Ihren AWS DataSync Agenten so konfigurieren, dass er mehrere Netzwerkadapter (NICs) verwendet, kann über mehr als eine IP-Adresse auf den Agenten zugegriffen werden. Dies kann in den folgenden Situationen wünschenswert sein:

- Maximierung des Durchsatzes — Möglicherweise möchten Sie den Durchsatz für einen Agenten maximieren, wenn Netzwerkadapter einen Engpass darstellen.
- Netzwerkisolierung — Ihr Network File System (NFS), Server Message Block (SMB), Hadoop Distributed File System (HDFS) oder Objektspeicherserver befinden sich möglicherweise in einem virtuellen LAN (VLAN), das aus Sicherheitsgründen keine Internetverbindung hat.

In einem typischen Anwendungsfall mit mehreren Adaptern wird ein Adapter als Route konfiguriert, über die der Agent kommuniziert (als Standardagent). AWS Mit Ausnahme dieses einen Adapters müssen sich NFS-, SMB-, HDFS- oder selbstverwaltete Objektspeicherorte im selben Subnetz befinden wie der Adapter, der eine Verbindung zu ihnen herstellt.

Andernfalls ist die Kommunikation mit den vorgesehenen NFS-, SMB-, HDFS- oder Objektspeicherorten möglicherweise nicht möglich. In einigen Fällen können Sie einen NFS-, SMB-, HDFS- oder Objektspeicherort auf demselben Adapter konfigurieren, der für die Kommunikation mit verwendet wird. AWS In diesen Fällen fließt der NFS-, SMB-, HDFS- oder Objektspeicherverkehr für diesen Server und AWS der Datenverkehr über denselben Adapter.

In einigen Fällen können Sie einen Adapter für die Verbindung mit der AWS DataSync Konsole konfigurieren und dann einen zweiten Adapter hinzufügen. In einem solchen Fall konfiguriert die Routing-Tabelle DataSync automatisch so, dass der zweite Adapter als bevorzugte Route verwendet wird.

Übertragung Ihrer Daten mit AWS DataSync

Mit AWS DataSync können Sie Daten zu oder von Speichern übertragen, die sich vor Ort AWS, in oder in anderen Clouds befinden.

Die Einrichtung einer DataSync Übertragung umfasst im Allgemeinen die folgenden Schritte:

1. Stellen Sie fest, ob [Ihre Übertragung DataSync unterstützt](#) wird.
2. Wenn [Sie einen DataSync Agenten für Ihre Übertragung benötigen](#), setzen Sie einen Agenten so nah wie möglich an einem Ihrer Speichersysteme ein und aktivieren Sie ihn.

Wenn Sie beispielsweise Daten von einem lokalen NFS-Dateiserver (Network File System) übertragen, setzen Sie den Agenten so nah wie möglich an diesem Dateiserver ein.

3. Gewähren Sie DataSync Zugriff auf Ihr Speichersystem.

DataSync benötigt die Erlaubnis, von Ihrem Speicher zu lesen oder in ihn zu schreiben (je nachdem, ob es sich bei Ihrem Speicher um einen Quell- oder Zielort handelt). Erfahren Sie beispielsweise, wie Sie [DataSync Zugriff auf NFS-Dateiserver gewähren](#).

4. [Connect Sie Ihr Netzwerk](#) für den Verkehr zwischen Ihrem Speichersystem und DataSync.
5. Erstellen Sie mithilfe der DataSync Konsole oder DataSync API einen Speicherort für Ihr Quellspeichersystem. AWS CLI

Erfahren Sie beispielsweise, wie Sie [einen NFS-Standort oder einen Amazon S3 S3-Standort erstellen](#).

6. Wiederholen Sie die Schritte 3 bis 5, um den Zielort Ihrer Übertragung zu erstellen.
7. [Erstellen und starten Sie eine DataSync Übertragungsaufgabe](#), die Ihre Quell- und Zielorte umfasst.

Themen

- [Mit wem kann ich meine Daten übertragen AWS DataSync?](#)
- [Übertragung zu oder von einem lokalen Speicher mit AWS DataSync](#)
- [Übertragung in oder aus dem AWS Speicher mit AWS DataSync](#)
- [Übertragung zu oder von einem anderen Cloud-Speicher mit AWS DataSync](#)
- [Eine Aufgabe für die Übertragung Ihrer Daten erstellen](#)
- [Eine Aufgabe zur Übertragung Ihrer Daten starten](#)

Mit wem kann ich meine Daten übertragen AWS DataSync?

Wohin Sie Ihre Daten übertragen können, AWS DataSync hängt von den folgenden Faktoren ab:

- Die Quell- und [Zielorte](#) Ihrer Übertragung
- Wenn sich Ihre Standorte an unterschiedlichen Orten befinden AWS-Konten
- Wenn sich Ihre Standorte an unterschiedlichen Orten befinden AWS-Regionen
- Wenn Sie den Basismodus oder den erweiterten Modus verwenden

Unterstützte Übertragungen im selben AWS-Konto

DataSync unterstützt Übertragungen zwischen den folgenden Speicherressourcen, die derselben zugeordnet sind AWS-Konto.

Quelle	Ziel	Erfordert einen Agenten?	Unterstützter Task-Modus
• NFS • SMB	• Amazon S3	Ja	Einfach, erweitert
• NFS • SMB	• Amazon EFS • Amazon FSx	Ja	Nur Basic
• HDFS • Objektspeicher	• Amazon S3 • Amazon EFS • Amazon FSx	Ja	Nur Basic
• Anderer Cloud-Speicher	• Amazon S3	Nur für den Basismodus	Einfach, erweitert
• Anderer Cloud-Speicher	• Amazon EFS • Amazon FSx	Ja	Nur Basic
• Amazon S3	• Amazon S3	Nein	Einfach, erweitert
• Amazon S3	• Amazon EFS	Nein	Nur Basic

Quelle	Ziel	Erfordert einen Agenten?	Unterstützter Task-Modus
	• Amazon FSx		
• Amazon S3	• NFS • SMB	Ja	Einfach, erweitert
• Amazon S3	• HDFS • Objektspeicher	Ja	Nur Basic
• Amazon S3	• Anderer Cloud-Speicher	Nur für den Basismodus	Einfach, erweitert
• Amazon EFS • Amazon FSx	• NFS • SMB	Ja	Nur Basic
• Amazon EFS • Amazon FSx	• HDFS • Objektspeicher	Ja	Nur Basic
• Amazon EFS • Amazon FSx	• Anderer Cloud-Speicher	Ja	Nur Basic
• Amazon EFS • Amazon FSx	• Amazon S3	Nein	Nur Basic
• Amazon EFS • Amazon FSx	• Amazon EFS • Amazon FSx	Nein	Nur Basic
• S3 on Outposts	• S3 (rein AWS-Regionen)	Ja	Nur Basic
• Amazon S3 (rein AWS-Regionen)	• S3 on Outposts	Ja	Nur Basic

Unterstützte Übertragungen zwischen AWS-Konten

DataSync unterstützt einige Übertragungen zwischen Speicherressourcen, die verschiedenen zugeordnet sind AWS-Konten.

Quelle	Ziel	Erfordert einen Agenten?	Unterstützter Task-Modus
- NFS - SMB	Amazon S3	Ja	Einfach, erweitert
- HDFS - Objektspeicher	Amazon S3	Ja	Nur Basic
Amazon S3	Amazon S3	Nein	Einfach, erweitert
Amazon S3	- Amazon EFS - Amazon FSx	Nein	Nur Basic
Amazon S3	- NFS - SMB	Ja	Einfach, erweitert
Amazon S3	- HDFS - Objektspeicher	Ja	Nur Basic
- Amazon EFS - Amazon FSx	Amazon S3	Nein	Nur Basic
- Amazon EFS¹ - Amazon FSx für OpenZFS¹ - Amazon FSx für Windows-Datenserver² - Amazon FSx für NetApp ONTAP³	- Amazon EFS - Amazon FSx	Ja (wenn als NFS/SMB Standort verwendet)	Nur Basic

- ¹ Als [NFS-Standort](#) konfiguriert.
- ² Als [SMB-Standort](#) konfiguriert.
- ³ Als NFS- oder SMB-Standort konfiguriert.

Unterstützte Übertragungen im selben AWS-Region

Es gibt keine Einschränkungen bei der Übertragung von Daten innerhalb derselben Regionen AWS-Region (einschließlich [optionaler Regionen](#)). Weitere Informationen finden Sie unter [AWS-Regionen unterstützt von DataSync](#).

Unterstützte Übertragungen zwischen AWS-Regionen

Beachten Sie Folgendes bei der Übertragung von Daten zwischen, die [AWS-Regionen unterstützt werden von DataSync](#):

- Bei der Übertragung zwischen AWS Speicherdiensten an verschiedenen AWS-Regionen Orten muss sich einer der beiden Standorte in der Region befinden, die Sie verwenden DataSync.
- Sie können keine Übertragung zwischen Regionen mit einem NFS-, SMB-, HDFS- oder Objektspeicherort durchführen. In diesen Situationen müssen sich Ihre beiden Übertragungsorte in derselben Region befinden, in der Sie Ihren Agenten [aktivieren](#). DataSync
- Mit AWS GovCloud (US) Regionen können Sie:
 - Transfer zwischen den Regionen AWS GovCloud (US-Ost) und AWS GovCloud (US-West).
 - Transfer zwischen einer AWS GovCloud (US) Region und einer kommerziellen Region AWS-Region, z. B. USA Ost (Nord-Virginia). Für diese Art der Übertragung ist bei der Übertragung zwischen Amazon EFS- oder FSx Amazon-Dateisystemen ein [Agent](#) erforderlich.

Important

Sie zahlen für die Datenübertragung zwischen AWS-Regionen. Diese Übertragung wird als Datenübertragung von der Quell- zur Zielregion abgerechnet. Weitere Informationen finden Sie unter [AWS DataSync – Preise](#).

Stellen Sie fest, ob für Ihre Übertragung ein Agent erforderlich ist DataSync

Abhängig von Ihrem Übertragungsszenario benötigen Sie möglicherweise einen DataSync Agenten. Weitere Informationen finden Sie unter [Brauche ich einen AWS DataSync Agenten?](#).

Übertragung zu oder von einem lokalen Speicher mit AWS DataSync

Mit AWS DataSync können Sie Dateien und Objekte zwischen einer Reihe von lokalen oder selbstverwalteten Speichersystemen und den folgenden Speicherdiensten übertragen: AWS

- [Amazon S3](#)
- [Amazon EFS](#)
- [Amazon FSx für Windows-Dateiserver](#)
- [Amazon FSx für Lustre](#)
- [Amazon FSx für OpenZFS](#)
- [Amazon FSx für NetApp ONTAP](#)

Themen

- [Konfiguration von AWS DataSync Übertragungen mit einem NFS-Dateiserver](#)
- [Konfiguration von AWS DataSync Übertragungen mit einem SMB-Dateiserver](#)
- [Konfiguration von AWS DataSync Übertragungen mit einem HDFS-Cluster](#)
- [Konfiguration von DataSync Übertragungen mit einem Objektspeichersystem](#)

Konfiguration von AWS DataSync Übertragungen mit einem NFS-Dateiserver

Mit AWS DataSync können Sie Daten zwischen Ihrem Network File System (NFS) -Dateiserver und den folgenden AWS Speicherdiensten übertragen. Die unterstützten Speicherdienste hängen von Ihrem Aufgabenmodus ab, wie unten dargestellt:

Basismodus	Verbesserter Modus
• Amazon S3	• Amazon S3

Basismodus	Verbesserter Modus
• Amazon EFS • Amazon FSx für Windows-Dateiserver • Amazon FSx für Lustre • Amazon FSx für OpenZFS • Amazon FSx für NetApp ONTAP	

Um diese Art der Übertragung einzurichten, erstellen Sie einen [Speicherort](#) für Ihren NFS-Dateiserver. Sie können diesen Speicherort als Übertragungsquelle oder -ziel verwenden.

Bereitstellung des DataSync Zugriffs auf NFS-Dateiserver

[Für DataSync den Zugriff auf Ihren NFS-Dateiserver benötigen Sie einen DataSync Agenten.](#) Der Agent mountet mithilfe des NFS-Protokolls einen Export auf Ihrem Dateiserver. Stellen Sie sicher, dass Sie den Agenten verwenden, der Ihrem gewünschten Aufgabenmodus entspricht.

Themen

- [Konfiguration Ihres NFS-Exports](#)
- [Unterstützte NFS-Versionen](#)

Konfiguration Ihres NFS-Exports

Welcher Export für Ihre Übertragung DataSync erforderlich ist, hängt davon ab, ob es sich bei Ihrem NFS-Dateiserver um einen Quell- oder Zielspeicherort handelt und wie die Berechtigungen Ihres Dateiservers konfiguriert sind.

Wenn es sich bei Ihrem Dateiserver um einen Quellspeicherort handelt, müssen Sie DataSync lediglich Ihre Dateien und Ordner lesen und durchqueren. Wenn es sich um einen Zielort handelt, DataSync benötigt er Root-Zugriff, um in den Speicherort zu schreiben und Besitzrechte, Berechtigungen und andere Metadaten für die Dateien und Ordner, die Sie kopieren, festzulegen. Sie können die `no_root_squash` Option verwenden, um Root-Zugriff für Ihren Export zu gewähren.

In den folgenden Beispielen wird beschrieben, wie Sie einen NFS-Export konfigurieren, der Zugriff DataSync auf ermöglicht.

Wenn Ihr NFS-Dateiserver ein Quellspeicherort ist (Root-Zugriff)

Konfigurieren Sie Ihren Export mithilfe des folgenden Befehls, der DataSync nur Leseberechtigungen (ro) und Root-Zugriff () gewährt: `no_root_squash`

```
export-path datasync-agent-ip-address(ro,no_root_squash)
```

Wenn Ihr NFS-Dateiserver ein Zielort ist

Konfigurieren Sie Ihren Export mithilfe des folgenden Befehls, der DataSync Schreibberechtigungen (rw) und Root-Zugriff (`no_root_squash`) bereitstellt:

```
export-path datasync-agent-ip-address(rw,no_root_squash)
```

Wenn Ihr NFS-Dateiserver ein Quellverzeichnis ist (kein Root-Zugriff)

Konfigurieren Sie Ihren Export mithilfe des folgenden Befehls, der die POSIX-Benutzer-ID (UID) und Gruppen-ID (GID) angibt, von denen Sie wissen, dass sie nur DataSync Leseberechtigungen für den Export gewähren würden:

```
export-path datasync-agent-ip-address(ro,all_squash,anonuid=uid,anongid=gid)
```

Unterstützte NFS-Versionen

DataSync Verwendet standardmäßig NFS-Version 4.1. DataSync unterstützt auch NFS 4.0 und 3.x.

Konfiguration Ihres Netzwerks für NFS-Übertragungen

Für Ihre DataSync Übertragung müssen Sie den Verkehr für einige Netzwerkverbindungen konfigurieren:

1. Erlauben Sie Datenverkehr über die folgenden Ports von Ihrem DataSync Agenten zu Ihrem NFS-Dateiserver:
 - Für NFS-Versionen 4.1 und 4.0 — TCP-Port 2049
 - Für NFS-Version 3.x — TCP-Ports 111 und 2049

Andere NFS-Clients in Ihrem Netzwerk sollten in der Lage sein, den NFS-Export zu mounten, den Sie für die Datenübertragung verwenden. Der Export muss auch ohne Kerberos-Authentifizierung zugänglich sein.

2. Konfigurieren Sie den Datenverkehr für Ihre [Service-Endpunktverbindung](#) (z. B. einen VPC-, öffentlichen oder FIPS-Endpunkt).
3. Erlauben Sie Datenverkehr vom DataSync Service zum [AWS Speicherservice](#), zu dem oder von dem Sie übertragen.

Erstellen Sie Ihren NFS-Übertragungsort

Bevor Sie beginnen, beachten Sie Folgendes:

- Sie benötigen einen NFS-Dateiserver, von dem Sie Daten übertragen möchten.
- Sie benötigen einen DataSync Agenten, der [auf Ihren Dateiserver zugreifen](#) kann.
- DataSync unterstützt nicht das Kopieren von NFS Version 4-Zugriffskontrolllisten (ACLs).

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp die Option Network File System (NFS) aus.
4. Wählen Sie für Agenten den DataSync Agenten aus, der eine Verbindung zu Ihrem NFS-Dateiserver herstellen kann.

Sie können mehr als einen Agenten auswählen. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

5. Geben Sie für NFS-Server den DNS-Namen (Domain Name System) oder die IP-Adresse des NFS-Dateiservers ein, mit dem Ihr DataSync Agent eine Verbindung herstellt.
6. Geben Sie unter Bereitstellungspfad den NFS-Exportpfad ein, den Sie mounten möchten DataSync .

Dieser Pfad (oder ein Unterverzeichnis des Pfads) ist der Ort, an den Daten DataSync übertragen werden oder von diesem Pfad. Weitere Informationen finden Sie unter [Konfiguration Ihres NFS-Exports](#).

7. (Optional) Erweitern Sie Zusätzliche Einstellungen und wählen Sie eine bestimmte NFS-Version aus, die Sie beim Zugriff auf Ihren Dateiserver verwenden möchten. DataSync

Weitere Informationen finden Sie unter [Unterstützte NFS-Versionen](#).

8. (Optional) Wählen Sie Tag hinzufügen, um Ihren NFS-Speicherort zu kennzeichnen.

Tags sind Schlüssel-Wert-Paare, mit denen Sie Ihre Standorte verwalten, filtern und nach ihnen suchen können. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

9. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

- Verwenden Sie den folgenden Befehl, um einen NFS-Speicherort zu erstellen.

```
aws datasync create-location-nfs \  
  --server-hostname nfs-server-address \  
  --on-prem-config AgentArns=datasync-agent-arns \  
  --subdirectory nfs-export-path
```

Weitere Informationen zum Erstellen des Speicherorts finden Sie unter [Bereitstellung des DataSync Zugriffs auf NFS-Dateiserver](#).

DataSync wählt automatisch die NFS-Version aus, die zum Lesen von einem NFS-Speicherort verwendet wird. Um eine NFS-Version anzugeben, verwenden Sie in der API-Operation [NfsMountOptions](#) den optionalen Parameter `Version`.

Dieser Befehl gibt für den NFS-Speicherort einen Amazon-Ressourcennamen (ARN) ähnlich dem folgenden ARN zurück.

```
{  
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/  
loc-0f01451b140b2af49"  
}
```

Um zu überprüfen, ob das Verzeichnis gemountet werden kann, können Sie eine Verbindung zu einem Computer mit der gleichen Netzwerkkonfiguration wie Ihr Agent herstellen und den folgenden CLI-Befehl ausführen.

```
mount -t nfs -o nfsvers=<nfs-server-version <nfs-server-address:<nfs-export-path <test-  
folder
```

Im Folgenden finden Sie ein Beispiel für den Befehl.


```
mount -t nfs -o nfsvers=3 198.51.100.123:/path_for_sync_to_read_from /  
temp_folder_to_test_mount_on_local_machine
```

Konfiguration von AWS DataSync Übertragungen mit einem SMB-Dateiserver

Mit AWS DataSync können Sie Daten zwischen Ihrem Server Message Block (SMB) -Dateiserver und den folgenden AWS Speicherdiensten übertragen. Die unterstützten Speicherdienste hängen von Ihrem Aufgabenmodus ab, wie unten dargestellt:

Basismodus	Verbesserter Modus
• Amazon S3 • Amazon EFS • Amazon FSx für Windows-Dateiserver • Amazon FSx für Lustre • Amazon FSx für OpenZFS • Amazon FSx für NetApp ONTAP	• Amazon S3

Um diese Art der Übertragung einzurichten, erstellen Sie einen [Speicherort](#) für Ihren SMB-Dateiserver. Sie können dies als Übertragungsquelle oder -ziel verwenden. Stellen Sie sicher, dass Sie den Agenten verwenden, der Ihrem gewünschten Aufgabenmodus entspricht.

Bereitstellung des DataSync Zugriffs auf SMB-Dateiserver

DataSync stellt über das SMB-Protokoll eine Verbindung zu Ihrem Dateiserver her und kann sich mit NTLM oder Kerberos authentifizieren.

Themen

- [Unterstützte SMB-Versionen](#)
- [Verwenden der NTLM-Authentifizierung](#)
- [Verwenden der Kerberos-Authentifizierung](#)
- [Erforderliche Berechtigungen](#)
- [DFS-Namespaces](#)

Unterstützte SMB-Versionen

Wählt standardmäßig DataSync automatisch eine Version des SMB-Protokolls auf der Grundlage der Verhandlungen mit Ihrem SMB-Dateiserver aus.

Sie können auch die Verwendung einer bestimmten SMB-Version konfigurieren. Wir empfehlen jedoch, dies nur dann DataSync zu tun, wenn DataSync Probleme bei der automatischen Aushandlung mit dem SMB-Dateiserver auftreten. DataSync unterstützt SMB-Versionen 1.0 und höher. Aus Sicherheitsgründen empfehlen wir die Verwendung von SMB Version 3.0.2 oder höher. Frühere Versionen, wie SMB 1.0, enthalten bekannte Sicherheitslücken, die Angreifer ausnutzen können, um Ihre Daten zu gefährden.

In der folgenden Tabelle finden Sie eine Liste der Optionen in der DataSync Konsole und der API:

Konsolenoption	API-Option	Description
Automatisch	AUTOMATIC	DataSync und der SMB-Dateiserver handeln zwischen 2.1 und 3.1.1 die höchste Version von SMB aus, die sie gegenseitig unterstützen. Dies ist die Standardoption und die empfohlene Option. Wenn Sie stattdessen eine bestimmte Version auswählen , die Ihr Dateiserver nicht unterstützt, erhalten Sie möglicherweise eine <code>Operation Not Supported</code> - Fehlermeldung.
SMB 3.0.2	SMB3	Beschränkt die Protokollaushandlung nur auf SMB-Version 3.0.2.
SMB 2.1	SMB2	Beschränkt die Protokollaushandlung nur auf SMB-Version 2.1.
SMB 2.0	SMB2_0	Beschränkt die Protokollaushandlung nur auf SMB Version 2.0.
SMB 1.0	SMB1	Beschränkt die Protokollaushandlung nur auf SMB Version 1.0.

Verwenden der NTLM-Authentifizierung

Um die NTLM-Authentifizierung zu verwenden, geben Sie einen Benutzernamen und ein Passwort an, mit denen Sie auf den SMB-Dateiserver zugreifen können, DataSync zu dem oder von dem Sie Daten übertragen. Der Benutzer kann ein lokaler Benutzer auf Ihrem Dateiserver oder ein Domänenbenutzer in Ihrem Microsoft Active Directory sein.

Verwenden der Kerberos-Authentifizierung

Um die Kerberos-Authentifizierung zu verwenden, stellen Sie einen Kerberos-Prinzipal, eine Kerberos-Schlüsseltabellendatei (Keytab) und eine Kerberos-Konfigurationsdatei bereit, die den Zugriff auf den SMB-Dateiserver ermöglichen, DataSync zu dem oder von dem Sie übertragen.

Themen

- [Voraussetzungen](#)
- [DataSync Konfigurationsoptionen für Kerberos](#)

Voraussetzungen

Sie müssen einige Kerberos-Artefakte erstellen und Ihr Netzwerk so konfigurieren, dass es auf Ihren SMB-Dateiserver zugreifen kann. DataSync

- [Erstellen Sie mithilfe des Dienstprogramms ktpass oder kutil eine Kerberos-Keytab-Datei.](#)

Im folgenden Beispiel wird eine Keytab-Datei mithilfe von erstellt. ktpass Der Kerberos-Bereich, den Sie angeben (MYDOMAIN.ORG), muss in Großbuchstaben geschrieben werden.

```
ktpass /out C:\YOUR_KEYTAB.keytab /princ HOST/kerberosuser@MYDOMAIN.ORG /mapuser  
kerberosuser /pass * /crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL
```

- Bereiten Sie eine vereinfachte Version der Kerberos-Konfigurationsdatei vor (). `krb5.conf` Fügen Sie Informationen über den Bereich, den Standort der Domain-Admin-Server und Zuordnungen von Hostnamen zu einem Kerberos-Bereich hinzu.

Stellen Sie sicher, dass der `krb5.conf` Inhalt mit der richtigen Groß- und Kleinschreibung für die Namen der Bereiche und Domänenbereiche formatiert ist. Beispiel:

```
[libdefaults]  
    dns_lookup_realm = true
```

```

dns_lookup_kdc = true
forwardable = true
default_realm = MYDOMAIN.ORG

[realms]
MYDOMAIN.ORG = {
    kdc = mydomain.org
    admin_server = mydomain.org
}

[domain_realm]
.mydomain.org = MYDOMAIN.ORG
mydomain.org = MYDOMAIN.ORG

```

- Stellen Sie in Ihrer Netzwerkkonfiguration sicher, dass Ihr Kerberos Key Distribution Center (KDC) - Serverport geöffnet ist. Der KDC-Port ist in der Regel der TCP-Port 88.

DataSync Konfigurationsoptionen für Kerberos

Wenn Sie einen SMB-Standort erstellen, der Kerberos verwendet, konfigurieren Sie die folgenden Optionen.

Konsolenoption	API-Option	Description
SMB-Server	ServerHostName	Der Domainname des SMB-Dateiservers, den Ihr DataSync Agent mounten wird. Für Kerberos können Sie die IP-Adresse des Dateiservers nicht angeben.
Kerberos-Prinzipal	KerberosPrincipal	Eine Identität in Ihrem Kerberos-Bereich, die berechtigt ist, auf die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver zuzugreifen. Ein Kerberos-Prinzipal könnte so aussehen. HOST/kerb

Konsolenoption	API-Option	Description
		<code>erouser@MYDOMAIN.ORG</code> Bei Prinzipalnamen wird Groß- und Kleinschreibung beachtet.
Keytab-Datei	KerberosKeytab	Eine Kerberos-Schlüssel tabellendatei (Keytab), die Zuordnungen zwischen Ihrem Kerberos-Prinzipal und den Verschlüsselungsschlüsseln enthält.
Kerberos-Konfigurationsdatei	KerberosKrbConf	Eine <code>krb5.conf</code> Datei, die Ihre Kerberos-Realm-Konfiguration definiert.
DNS-IP-Adressen (optional)	DnsIpAddresses	Die IPv4 Adressen für die DNS-Server, zu denen Ihr SMB-Dateiserver gehört. Wenn Sie mehrere Domänen in Ihrer Umgebung haben, stellen Sie durch diese Konfiguration sicher, dass DataSync eine Verbindung zum richtigen SMB-Dateiserver hergestellt wird.

Erforderliche Berechtigungen

Die von Ihnen angegebene Identität DataSync muss berechtigt sein, die Dateien, Ordner und Dateimetadaten Ihres SMB-Dateiservers bereitzustellen und darauf zuzugreifen.

Wenn Sie in Ihrem Active Directory eine Identität angeben, muss diese Mitglied einer Active Directory-Gruppe mit einem oder beiden der folgenden Benutzerrechte sein (abhängig von den [Metadaten, die Sie kopieren DataSync möchten](#)):

Benutzerrecht	Description
Dateien und Verzeichnisse wiederherstellen (SE_RESTORE_NAME)	Ermöglicht DataSync das Kopieren von Objekteigenthümern, Berechtigungen, Dateimetadaten und beliebigen NTFS-Zugriffslisten (DACLs). Dieses Benutzerrecht wird normalerweise Mitgliedern der Gruppen Domänen-Admins und Backup-Operatoren gewährt (beide sind Active Directory-Standardgruppen).
Überwachungs- und Sicherheitsprotokoll verwalten () SE_SECURITY_NAME	Ermöglicht DataSync das Kopieren von NTFS-Systemzugriffskontrolllisten (SACLs). Dieses Benutzerrecht wird normalerweise Mitgliedern der Gruppe Domänen-Admins gewährt.

Wenn Sie Windows kopieren möchten ACLs und zwischen einem SMB-Dateiserver und einem anderen Speichersystem, das SMB verwendet (wie Amazon FSx für Windows File Server oder FSx für ONTAP), übertragen, DataSync muss die von Ihnen angegebene Identität zu derselben Active Directory-Domäne gehören oder über eine Active Directory-Vertrauensstellung zwischen ihren Domänen verfügen.

DFS-Namespaces

DataSync unterstützt keine Microsoft Distributed File System (DFS) -Namespaces. Wir empfehlen, bei der Erstellung Ihres Standorts stattdessen einen zugrunde liegenden Dateiserver oder eine Dateifreigabe anzugeben. DataSync

Erstellen Sie Ihren SMB-Übertragungsort

Bevor Sie beginnen, benötigen Sie einen SMB-Dateiserver, von dem Sie Daten übertragen möchten.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter. <https://console.aws.amazon.com/datasync/>

2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie für Location type (Speicherorttyp) Server Message Block (SMB).

Sie konfigurieren diesen Speicherort später als Quelle oder Ziel.

4. Wählen Sie für Agenten den DataSync Agenten aus, der eine Verbindung zu Ihrem SMB-Dateiserver herstellen kann.

Sie können mehr als einen Agenten auswählen. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

5. Geben Sie für SMB-Server den Domainnamen oder die IP-Adresse des SMB-Dateiservers ein, den Ihr DataSync Agent bereitstellen wird.

Beachten Sie bei dieser Einstellung Folgendes:

- Sie können keine IP-Adresse der Version 6 (IPv6) angeben.
 - Wenn Sie die Kerberos-Authentifizierung verwenden, müssen Sie einen Domännennamen angeben.
6. Geben Sie unter Freigabename den Namen der Freigabe ein, die von Ihrem SMB-Dateiserver exportiert wurde und auf der Daten gelesen oder DataSync geschrieben werden sollen.

Sie können ein Unterverzeichnis in den Freigabepfad aufnehmen (z. B. /path/to/subdirectory). Stellen Sie sicher, dass andere SMB-Clients in Ihrem Netzwerk diesen Pfad ebenfalls bereitstellen können.

Um alle Daten im Unterverzeichnis zu kopieren, DataSync müssen Sie in der Lage sein, die SMB-Freigabe zu mounten und auf alle zugehörigen Daten zuzugreifen. Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

7. (Optional) Erweitern Sie Zusätzliche Einstellungen und wählen Sie eine SMB-Version aus, die Sie beim Zugriff auf Ihren Dateiserver verwenden möchten. DataSync

Wählt standardmäßig DataSync automatisch eine Version aus, die auf Verhandlungen mit dem SMB-Dateiserver basiert. Weitere Informationen finden Sie unter [Unterstützte SMB-Versionen](#).

8. Wählen Sie als Authentifizierungstyp NTLM oder Kerberos aus.
9. Führen Sie je nach Authentifizierungstyp einen der folgenden Schritte aus:

NTLM

- Geben Sie unter Benutzer einen Benutzernamen ein, der Ihren SMB-Dateiserver einbinden kann und der Zugriff auf die Dateien und Ordner hat, die an Ihrer Übertragung beteiligt sind.

Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

- Geben Sie unter Passwort das Passwort des Benutzers ein, der Ihren SMB-Dateiserver mounten kann und Zugriff auf die Dateien und Ordner hat, die an Ihrer Übertragung beteiligt sind.
- (Optional) Geben Sie unter Domain den Windows-Domänennamen ein, zu dem Ihr SMB-Dateiserver gehört.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieser Einstellung sichergestellt, dass DataSync eine Verbindung zum richtigen SMB-Dateiserver hergestellt wird.

Kerberos

- Geben Sie für Kerberos-Prinzipal einen Prinzipal in Ihrem Kerberos-Bereich an, der berechtigt ist, auf die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver zuzugreifen.

Ein Kerberos-Prinzipal könnte wie folgt aussehen. `HOST/kerberosuser@MYDOMAIN.ORG`

Bei Prinzipalnamen wird Groß- und Kleinschreibung beachtet. Ihre DataSync Aufgabenausführung schlägt fehl, wenn der Prinzipal, den Sie für diese Einstellung angeben, nicht exakt mit dem Prinzipal übereinstimmt, den Sie zum Erstellen der Keytab-Datei verwenden.

- Laden Sie für die Keytab-Datei eine Keytab-Datei hoch, die Zuordnungen zwischen Ihrem Kerberos-Prinzipal und den Verschlüsselungsschlüsseln enthält.
- Laden Sie für die Kerberos-Konfigurationsdatei eine **krb5.conf** Datei hoch, die Ihre Kerberos-Realm-Konfiguration definiert.
- (Optional) Geben Sie für DNS-IP-Adressen bis zu zwei IPv4 Adressen für die DNS-Server an, zu denen Ihr SMB-Dateiserver gehört.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen SMB-Dateiserver hergestellt wird.

10. (Optional) Wählen Sie Tag hinzufügen aus, um Ihren SMB-Standort zu kennzeichnen.

Stichwörter sind Schlüssel-Wert-Paare, die Ihnen helfen, Ihre Standorte zu verwalten, zu filtern und nach ihnen zu suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

11. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

In den folgenden Anweisungen wird beschrieben, wie SMB-Standorte mit NTLM- oder Kerberos-Authentifizierung erstellt werden.

NTLM

1. Kopieren Sie den folgenden Befehl. `create-location-smb`

```
aws datasync create-location-smb \
  --agent-arns datasync-agent-arns \
  --server-hostname smb-server-address \
  --subdirectory smb-export-path \
  --authentication-type "NTLM" \
  --user user-who-can-mount-share \
  --password user-password \
  --domain windows-domain-of-smb-server
```

2. Geben Sie für `--agent-arns` den DataSync Agenten an, der eine Verbindung zu Ihrem SMB-Dateiserver herstellen kann.

Sie können mehr als einen Agenten auswählen. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

3. Geben Sie für `--server-hostname` den Domainnamen oder die IPv4 Adresse des SMB-Dateiservers an, den Ihr DataSync Agent bereitstellen wird.
4. Geben Sie für den Namen der Freigabe an `--subdirectory`, die von Ihrem SMB-Dateiserver exportiert wurde und auf der Daten gelesen oder geschrieben DataSync werden sollen.

Sie können ein Unterverzeichnis in den Freigabepfad aufnehmen (z. B. `/path/to/subdirectory`). Stellen Sie sicher, dass andere SMB-Clients in Ihrem Netzwerk diesen Pfad ebenfalls bereitstellen können.

Um alle Daten im Unterverzeichnis zu kopieren, DataSync müssen Sie in der Lage sein, die SMB-Freigabe zu mounten und auf alle zugehörigen Daten zuzugreifen. Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

5. Geben Sie zum Beispiel einen Benutzernamen an `--user`, der Ihren SMB-Dateiserver einbinden kann und der Zugriff auf die Dateien und Ordner hat, die an Ihrer Übertragung beteiligt sind.

Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

6. Geben Sie zum `--password` Beispiel das Passwort des Benutzers an, der Ihren SMB-Dateiserver bereitstellen kann und über Zugriffsrechte auf die Dateien und Ordner verfügt, die an Ihrer Übertragung beteiligt sind.
7. (Optional) Geben Sie für `--domain` den Windows-Domännennamen an, zu dem Ihr SMB-Dateiserver gehört.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieser Einstellung sichergestellt, dass DataSync eine Verbindung zum richtigen SMB-Dateiserver hergestellt wird.

8. (Optional) Fügen Sie die `--version` Option hinzu, wenn Sie eine bestimmte SMB-Version verwenden möchten DataSync. Weitere Informationen finden Sie unter [Unterstützte SMB-Versionen](#).
9. Führen Sie den Befehl `create-location-smb` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN des Speicherorts anzeigt, den Sie erstellt haben. Beispiel:

```
{
  "arn:aws:datsync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Kerberos

1. Kopieren Sie den folgenden `create-location-smb` Befehl.

```
aws datasync create-location-smb \  
  --agent-arns datasync-agent-arns \  
  --server-hostname smb-server-address \  
  --subdirectory smb-export-path \  
  --authentication-type "KERBEROS" \  
  --kerberos-principal "HOST/kerberosuser@EXAMPLE.COM" \  
  --kerberos-keytab "file://path/to/file.keytab" \  
  --kerberos-krb5-conf "file://path/to/krb5.conf" \  
  --dns-ip-addresses array-of-ipv4-addresses
```

2. Geben Sie für `--agent-arns` den DataSync Agenten an, der eine Verbindung zu Ihrem SMB-Dateiserver herstellen kann.

Sie können mehr als einen Agenten auswählen. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

3. Geben Sie für `--server-hostname` den Domainnamen des SMB-Dateiservers an, den Ihr DataSync Agent bereitstellen wird.
4. Geben Sie für den Namen der Freigabe an `--subdirectory`, die von Ihrem SMB-Dateiserver exportiert wurde und auf der Daten gelesen oder geschrieben DataSync werden sollen.

Sie können ein Unterverzeichnis in den Freigabepfad aufnehmen (z. B. `/path/to/subdirectory`). Stellen Sie sicher, dass andere SMB-Clients in Ihrem Netzwerk diesen Pfad ebenfalls bereitstellen können.

Um alle Daten im Unterverzeichnis zu kopieren, DataSync müssen Sie in der Lage sein, die SMB-Freigabe zu mounten und auf alle zugehörigen Daten zuzugreifen. Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

5. Gehen Sie für die Kerberos-Optionen wie folgt vor:
 - `--kerberos-principal`: Geben Sie in Ihrem Kerberos-Bereich einen Prinzipal an, der berechtigt ist, auf die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver zuzugreifen.

Ein Kerberos-Prinzipal könnte wie folgt aussehen. `HOST/kerberosuser@MYDOMAIN.ORG`

Bei Prinzipalnamen wird Groß- und Kleinschreibung beachtet. Ihre DataSync Aufgabenausführung schlägt fehl, wenn der Prinzipal, den Sie für diese Option angeben, nicht exakt dem Prinzipal entspricht, den Sie zum Erstellen der Keytab-Datei verwenden.

- `--kerberos-keytab`: Geben Sie eine Keytab-Datei an, die Zuordnungen zwischen Ihrem Kerberos-Prinzipal und den Verschlüsselungsschlüsseln enthält.
- `--kerberos-krb5-conf`: Geben Sie eine `krb5.conf` Datei an, die Ihre Kerberos-Realm-Konfiguration definiert.
- (Optional) `--dns-ip-addresses`: Geben Sie bis zu zwei IPv4 Adressen für die DNS-Server an, zu denen Ihr SMB-Dateiserver gehört.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen SMB-Dateiserver hergestellt wird.

6. (Optional) Fügen Sie die `--version` Option hinzu, wenn Sie eine bestimmte SMB-Version verwenden möchten DataSync. Weitere Informationen finden Sie unter [Unterstützte SMB-Versionen](#).
7. Führen Sie den Befehl `create-location-smb` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN des Speicherorts anzeigt, den Sie erstellt haben. Beispiel:

```
{
  "arn:aws:datasync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Konfiguration von AWS DataSync Übertragungen mit einem HDFS-Cluster

Mit AWS DataSync können Sie mithilfe von Aufgaben im Basismodus Daten zwischen Ihrem Hadoop Distributed File System (HDFS) -Cluster und einem der folgenden AWS Speicherdienste übertragen:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Amazon FSx für Windows-Dateiserver](#)
- [Amazon FSx für Lustre](#)
- [Amazon FSx für OpenZFS](#)
- [Amazon FSx für NetApp ONTAP](#)

Um diese Art der Übertragung einzurichten, erstellen Sie einen [Speicherort](#) für Ihren HDFS-Cluster. Sie können diesen Standort als Übertragungsquelle oder -ziel verwenden.

Bereitstellung des DataSync Zugriffs auf HDFS-Cluster

Um eine Verbindung zu Ihrem HDFS-Cluster herzustellen, DataSync wird ein [Agent im Basismodus verwendet, den Sie so nah wie möglich an Ihrem HDFS-Cluster bereitstellen](#). Der DataSync Agent fungiert als HDFS-Client und kommuniziert mit dem NameNodes und DataNodes in Ihrem Cluster.

Wenn Sie eine Übertragungsaufgabe starten, werden die NameNode Speicherorte von Dateien und Ordnern auf dem Cluster DataSync abgefragt. Wenn Sie Ihren HDFS-Speicherort als Quellverzeichnis konfigurieren, DataSync liest Dateien und Ordnerdaten aus DataNodes dem Cluster und kopiert diese Daten an das Ziel. Wenn Sie Ihren HDFS-Speicherort als Zielspeicherort konfigurieren, werden dann Dateien und Ordner von der Quelle in den Ordner DataNodes in Ihrem Cluster DataSync geschrieben.

Authentifizierung

DataSync Unterstützt beim Herstellen einer Verbindung zu einem HDFS-Cluster die einfache Authentifizierung oder die Kerberos-Authentifizierung. Um die einfache Authentifizierung zu verwenden, geben Sie den Benutzernamen eines Benutzers mit Lese- und Schreibberechtigungen für den HDFS-Cluster an. Um die Kerberos-Authentifizierung zu verwenden, geben Sie eine Kerberos-Konfigurationsdatei, eine Kerberos-Schlüsseltabellendatei (Keytab) und einen Kerberos-Prinzipalnamen an. Die Anmeldeinformationen des Kerberos-Prinzipals müssen in der bereitgestellten Keytab-Datei enthalten sein.

Verschlüsselung

DataSync Unterstützt bei Verwendung der Kerberos-Authentifizierung die Verschlüsselung von Daten bei der Übertragung zwischen dem DataSync Agenten und Ihrem HDFS-Cluster. Verschlüsseln Sie Ihre Daten, indem Sie die QOP-Konfigurationseinstellungen (Quality of Protection) auf Ihrem HDFS-Cluster verwenden und die QOP-Einstellungen bei der Erstellung Ihres HDFS-Standorts angeben. Die QOP-Konfiguration umfasst Einstellungen für den Datenübertragungsschutz und den RPC-Schutz (Remote Procedure Call).

DataSync unterstützt die folgenden Kerberos-Verschlüsselungstypen:

- `des-cbc-crc`
- `des-cbc-md4`

- des-cbc-md5
- des3-cbc-sha1
- arcfour-hmac
- arcfour-hmac-exp
- aes128-cts-hmac-sha1-96
- aes256-cts-hmac-sha1-96
- aes128-cts-hmac-sha256-128
- aes256-cts-hmac-sha384-192
- camellia128-cts-cmac
- camellia256-cts-cmac

Sie können HDFS-Cluster auch für die Verschlüsselung im Ruhezustand mithilfe von Transparent Data Encryption (TDE) konfigurieren. Bei Verwendung der einfachen Authentifizierung werden DataSync Lese- und Schreibvorgänge in TDE-fähige Cluster ausgeführt. Wenn Sie Daten in einen TDE-fähigen Cluster kopieren DataSync möchten, konfigurieren Sie zunächst die Verschlüsselungszonen auf dem HDFS-Cluster. DataSync erstellt keine Verschlüsselungszonen.

HDFS-Funktionen werden nicht unterstützt

Die folgenden HDFS-Funktionen werden derzeit nicht unterstützt von: DataSync

- Transparente Datenverschlüsselung (TDE) bei Verwendung der Kerberos-Authentifizierung
- Konfiguration mehrerer NameNodes
- Hadoop HDFS über HTTP (HttpFS)
- POSIX-Zugriffskontrolllisten () ACLs
- Erweiterte HDFS-Attribute (Xattrs)
- HDFS-Cluster, die Apache verwenden HBase

Erstellen Sie Ihren HDFS-Übertragungsort

Sie können Ihren Standort als Quelle oder Ziel für Ihre DataSync Übertragung verwenden.

Bevor Sie beginnen: Überprüfen Sie die Netzwerkkonnektivität zwischen Ihrem Agenten und dem Hadoop-Cluster, indem Sie wie folgt vorgehen:

- Testen Sie den Zugriff auf die unter aufgeführten TCP-Ports. [Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher](#)
- Testen Sie den Zugriff zwischen Ihrem lokalen Agenten und Ihrem Hadoop-Cluster. Detaillierte Anweisungen finden Sie unter [Überprüfen Sie die Verbindung Ihres Agenten zu Ihrem Speichersystem](#).

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter. <https://console.aws.amazon.com/datasync/>
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp die Option Hadoop Distributed File System (HDFS) aus.

Sie können diesen Speicherort später als Quelle oder Ziel konfigurieren.

4. Wählen Sie für Agents den Agenten aus, der eine Verbindung zu Ihrem HDFS-Cluster herstellen kann.

Sie können mehr als einen Agenten auswählen. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

5. Geben Sie für NameNodeden Domainnamen oder die IP-Adresse des primären NameNode HDFS-Clusters an.
6. Geben Sie unter Ordner einen Ordner auf Ihrem HDFS-Cluster ein, den Sie für die Datenübertragung verwenden DataSync möchten.

Wenn es sich bei Ihrem HDFS-Speicherort um eine Quelle handelt, werden die Dateien in diesem Ordner an das Ziel DataSync kopiert. Wenn es sich bei Ihrem Standort um ein Ziel handelt, werden Dateien in diesen Ordner DataSync geschrieben.

7. Um die Blockgröße oder den Replikationsfaktor festzulegen, wählen Sie Zusätzliche Einstellungen.

Die Standardblockgröße ist 128 MiB. Die von Ihnen angegebenen Blockgrößen müssen ein Vielfaches von 512 Byte sein.

DataNodes Bei der Übertragung auf den HDFS-Cluster ist der Standardreplikationsfaktor drei.

8. Wählen Sie im Abschnitt Sicherheit den Authentifizierungstyp aus, der auf Ihrem HDFS-Cluster verwendet wird.

- Einfach — Geben Sie für Benutzer den Benutzernamen mit den folgenden Berechtigungen auf dem HDFS-Cluster an (abhängig von Ihrem Anwendungsfall):
 - Wenn Sie diesen Speicherort als Quellspeicherort verwenden möchten, geben Sie einen Benutzer an, der nur über Leseberechtigungen verfügt.
 - Wenn Sie diesen Speicherort als Zielort verwenden möchten, geben Sie einen Benutzer mit Lese- und Schreibberechtigungen an.

Geben Sie optional den URI des Key Management Servers (KMS) Ihres HDFS-Clusters an.

- Kerberos — Geben Sie den Kerberos-Prinzipal mit Zugriff auf Ihren HDFS-Cluster an. Geben Sie als Nächstes die KeyTabDatei an, die den bereitgestellten Kerberos-Prinzipal enthält. Stellen Sie dann die Kerberos-Konfigurationsdatei bereit. Geben Sie abschließend die Art der Verschlüsselung beim Übertragungsschutz in den Dropdownlisten RPC-Schutz und Datenübertragungsschutz an.
9. (Optional) Wählen Sie Tag hinzufügen aus, um Ihren HDFS-Standort zu kennzeichnen.
- Tags sind Schlüssel-Wert-Paare, die Ihnen helfen, Ihre Standorte zu verwalten, zu filtern und nach ihnen zu suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.
10. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden `create-location-hdfs` Befehl.

```
aws datasync create-location-hdfs --name-nodes [{"Hostname":"host1", "Port": 8020}] \
  \
  --authentication-type "SIMPLE|KERBEROS" \
  --agent-arns [arn:aws:datasync:us-east-1:123456789012:agent/  
agent-01234567890example] \
  --subdirectory "/path/to/my/data"
```

2. Geben Sie für den `--name-nodes` Parameter den Hostnamen oder die IP-Adresse des primären HDFS-Clusters NameNode und den TCP-Port an, den der NameNode empfängt.
3. Geben Sie für den `--authentication-type` Parameter den Authentifizierungstyp an, der für die Verbindung mit dem Hadoop-Cluster verwendet werden soll. Sie können `SIMPLE` oder `KERBEROS` angeben.

Wenn Sie die SIMPLE Authentifizierung verwenden, verwenden Sie den `--simple-user` Parameter, um den Benutzernamen des Benutzers anzugeben. Wenn Sie die KERBEROS Authentifizierung verwenden, verwenden Sie die `--kerberos-krb5-conf` Parameter `--kerberos-principal` `--kerberos-keytab`, und. Weitere Informationen finden Sie unter [create-location-hdfs](#).

4. Geben Sie für den `--agent-arns` Parameter den ARN des DataSync Agenten an, der eine Verbindung zu Ihrem HDFS-Cluster herstellen kann.

Sie können mehr als einen Agenten auswählen. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

5. (Optional) Geben Sie für den `--subdirectory` Parameter einen Ordner auf Ihrem HDFS-Cluster DataSync an, den Sie für die Datenübertragung verwenden möchten.

Wenn es sich bei Ihrem HDFS-Speicherort um eine Quelle handelt, werden die Dateien in diesem Ordner an das Ziel DataSync kopiert. Wenn es sich bei Ihrem Standort um ein Ziel handelt, werden Dateien in diesen Ordner DataSync geschrieben.

6. Führen Sie den Befehl `create-location-hdfs` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN des Speicherorts anzeigt, den Sie erstellt haben. Beispiel:

```
{
  "arn:aws:datsync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Konfiguration von DataSync Übertragungen mit einem Objektspeichersystem

Mit AWS DataSync können Sie mithilfe von Aufgaben im Basismodus Daten zwischen Ihrem Objektspeichersystem und einem der folgenden AWS Speicherdienste übertragen:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Amazon FSx für Windows-Dateiserver](#)
- [Amazon FSx für Lustre](#)

- [Amazon FSx für OpenZFS](#)
- [Amazon FSx für NetApp ONTAP](#)

Um diese Art der Übertragung einzurichten, erstellen Sie einen [Speicherort](#) für Ihr Objektspeichersystem. Sie können diesen Speicherort als Übertragungsquelle oder -ziel verwenden. Für die Übertragung von Daten zu oder von Ihrem lokalen Objektspeicher ist ein DataSync Agent im Basismodus erforderlich.

Voraussetzungen

Ihr Objektspeichersystem muss mit den folgenden [Amazon S3 S3-API-Vorgängen](#) kompatibel sein DataSync , um eine Verbindung herzustellen:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetBucketLocation
- GetObject
- GetObjectTagging
- HeadBucket
- HeadObject
- ListObjectsV2
- PutObject
- PutObjectTagging
- UploadPart

Erstellen Sie Ihren Objektspeicher-Transferort

Bevor Sie beginnen, benötigen Sie ein Objektspeichersystem, zu dem Sie Daten übertragen möchten oder von dem Sie Daten übertragen möchten.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp die Option Objektspeicher aus.

Sie konfigurieren diesen Speicherort später als Quelle oder Ziel.

4. Geben Sie für Server den Domainnamen oder die IP-Adresse des Objektspeicherservers an.
5. Geben Sie als Bucket-Namen den Namen des Objektspeicher-Buckets ein, der an der Übertragung beteiligt ist.
6. Geben Sie für Ordner ein Objektpräfix ein.

DataSync kopiert nur Objekte mit diesem Präfix.

7. Wenn für Ihre Übertragung ein Agent erforderlich ist, wählen Sie Agenten verwenden und dann den DataSync Agenten aus, der eine Verbindung zu Ihrem Objektspeichersystem herstellt.

Für einige Übertragungen sind keine Agenten erforderlich. In anderen Szenarien möchten Sie möglicherweise mehr als einen Agenten verwenden. Weitere Informationen erhalten Sie unter [Situationen, in denen Sie keinen DataSync Agenten benötigen](#) und [Verwendung mehrerer DataSync Agenten](#).

8. Um die Verbindung zum Object Storage-Server zu konfigurieren, erweitern Sie Zusätzliche Einstellungen und gehen Sie wie folgt vor:
 - a. Wählen Sie als Serverprotokoll HTTP oder HTTPS aus.
 - b. Verwenden Sie als Serverport einen Standardport (80 für HTTP oder 443 für HTTPS) oder geben Sie bei Bedarf einen benutzerdefinierten Port an.
 - c. Wenn Ihr Objektspeichersystem eine private oder selbstsignierte Zertifizierungsstelle (CA) verwendet, wählen Sie unter Zertifikat die Option Datei auswählen und geben Sie eine einzelne **.pem** Datei mit einer vollständigen Zertifikatskette an.

Die Zertifikatskette könnte Folgendes beinhalten:

- Das Zertifikat des Objektspeichersystems
- Alle Zwischenzertifikate (falls vorhanden)
- Das Stammzertifikat der signierenden Zertifizierungsstelle

Sie können Ihre Zertifikate zu einer .pem Datei zusammenfügen (die vor der Base64-Kodierung bis zu 32768 Byte groß sein kann). Mit dem folgenden cat Beispielfehl wird eine `object_storage_certificates`.pem Datei erstellt, die drei Zertifikate enthält:

```
cat object_server_certificate.pem intermediate_certificate.pem ca_root_certificate.pem  
> object_storage_certificates.pem
```

9. Wenn der Objektspeicherserver Anmeldeinformationen für den Zugriff benötigt, wählen Sie Anmeldedaten erforderlich aus und geben Sie den Zugriffsschlüssel ein, den Sie für den Zugriff auf den Bucket verwenden. Geben Sie dann entweder den geheimen Schlüssel direkt ein oder geben Sie ein AWS Secrets Manager Geheimnis an, das den Schlüssel enthält. Weitere Informationen finden Sie unter [Bereitstellen von Anmeldeinformationen für Speicherorte](#).

Der Zugriffsschlüssel und der geheime Schlüssel können jeweils ein Benutzername und ein Passwort sein.

10. (Optional) Wählen Sie Tag hinzufügen aus, um Ihren Objektspeicherort zu kennzeichnen.

Tags sind Schlüssel-Wert-Paare, die Ihnen helfen, Ihre Standorte zu verwalten, zu filtern und nach ihnen zu suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

11. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden create-location-object-storage Befehl:

```
aws datasync create-location-object-storage \  
  --server-hostname object-storage-server.example.com \  
  --bucket-name your-bucket \  
  --agent-arns arn:aws:datasync:us-east-1:123456789012:agent/  
agent-01234567890deadfb
```

2. Geben Sie im Befehl die folgenden erforderlichen Parameter an:

- `--server-hostname`— Geben Sie den Domainnamen oder die IP-Adresse Ihres Objektspeicherservers an.

- `--bucket-name`— Geben Sie den Namen des Buckets auf Ihrem Objektspeicherserver an, zu dem oder von dem Sie Daten übertragen.
3. (Optional) Fügen Sie dem Befehl einen der folgenden Parameter hinzu:
- `--agent-arns`— Geben Sie die DataSync Agenten an, die Sie mit Ihrem Object Storage-Server verbinden möchten.
 - `--server-port`— Gibt den Port an, über den Ihr Objektspeicherserver eingehenden Netzwerkverkehr akzeptiert (z. B. Port443).
 - `--server-protocol`— Gibt das Protokoll (HTTPoderHTTPS) an, das Ihr Objektspeicherserver für die Kommunikation verwendet.
 - `--access-key`— Gibt den Zugriffsschlüssel (z. B. einen Benutzernamen) an, wenn Anmeldeinformationen für die Authentifizierung beim Objektspeicherserver erforderlich sind.
 - `--secret-key`— Gibt den geheimen Schlüssel (z. B. ein Passwort) an, wenn Anmeldeinformationen für die Authentifizierung beim Objektspeicherserver erforderlich sind.

Sie können auch zusätzliche Parameter für die Sicherung Ihrer Schlüssel angeben, indem AWS Secrets Manager Sie. Weitere Informationen finden Sie unter [Bereitstellen von Anmeldeinformationen für Speicherorte](#).

- `--server-certificate`— Gibt eine Zertifikatskette für DataSync die Authentifizierung bei Ihrem Objektspeichersystem an, falls das System eine private oder selbstsignierte Zertifizierungsstelle (CA) verwendet. Sie müssen eine einzelne .pem Datei mit einer vollständigen Zertifikatskette angeben (z. B. `file:///home/user/.ssh/object_storage_certificates.pem`).

Die Zertifikatskette könnte Folgendes beinhalten:

- Das Zertifikat des Objektspeichersystems
- Alle Zwischenzertifikate (falls vorhanden)
- Das Stammzertifikat der signierenden Zertifizierungsstelle

Sie können Ihre Zertifikate zu einer .pem Datei zusammenfügen (die vor der Base64-Kodierung bis zu 32768 Byte groß sein kann). Mit dem folgenden `cat` Beispielbefehl wird eine *object_storage_certificates*.pem Datei erstellt, die drei Zertifikate enthält:

```
cat object_server_certificate.pem intermediate_certificate.pem ca_root_certificate.pem  
> object_storage_certificates.pem
```

- `--subdirectory`— Gibt das Objektpräfix für Ihren Objektspeicherserver an.

DataSync kopiert nur Objekte mit diesem Präfix.

- `--tags`— Gibt das Schlüssel-Wert-Paar an, das ein Tag darstellt, das Sie der Standortressource hinzufügen möchten.

Mithilfe von Tags können Sie Ihre Ressourcen verwalten, filtern und suchen. Wir empfehlen, ein Namensschild für Ihren Standort zu erstellen.

4. Führen Sie den Befehl `create-location-object-storage` aus.

Sie erhalten eine Antwort, die Ihnen den Standort-ARN anzeigt, den Sie gerade erstellt haben.

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-01234567890abcdef"
}
```

Übertragung in oder aus dem AWS Speicher mit AWS DataSync

Mit AWS DataSync können Sie Daten zu oder von einer Reihe von AWS Speicherdiensten übertragen. Weitere Informationen finden Sie unter [Wo kann ich meine Daten übertragen DataSync?](#)

Themen

- [Konfiguration von AWS DataSync Übertragungen mit Amazon S3](#)
- [Konfiguration von AWS DataSync Übertragungen mit Amazon EFS](#)
- [Konfiguration von Übertragungen mit FSx für Windows File Server](#)
- [DataSync Transfers mit FSx for Lustre konfigurieren](#)
- [Konfiguration von DataSync Übertragungen mit Amazon FSx für OpenZFS](#)
- [Konfiguration von Übertragungen mit Amazon FSx für NetApp ONTAP](#)

Konfiguration von AWS DataSync Übertragungen mit Amazon S3

Um Daten zu oder von Ihrem Amazon S3 S3-Bucket zu übertragen, erstellen Sie einen AWS DataSync Übertragungsort. DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bereitstellung des DataSync Zugriffs auf S3-Buckets

DataSync benötigt Zugriff auf den S3-Bucket, in den oder von dem Sie übertragen. Dazu müssen Sie eine AWS Identity and Access Management (IAM-) Rolle erstellen, die über die für DataSync den Zugriff auf den Bucket erforderlichen Berechtigungen verfügt. Diese Rolle geben Sie dann an, wenn [Sie Ihren Amazon S3 S3-Standort für erstellen DataSync](#).

Inhalt

- [Erforderliche Berechtigungen](#)
- [Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort](#)
- [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#)
- [Zugriff auf eingeschränkte S3-Buckets](#)
- [Zugriff auf S3-Buckets mit eingeschränktem VPC-Zugriff](#)

Erforderliche Berechtigungen

Die Berechtigungen, die Ihre IAM-Rolle benötigt, können davon abhängen, ob es sich bei dem Bucket um einen DataSync Quell- oder Zielspeicherort handelt. Für Amazon S3 on Outposts sind andere Berechtigungen erforderlich.

Amazon S3 (source location)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
```

```

        "s3:ListMultipartUploadParts"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}

```

Amazon S3 (destination location)

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {

```



```

        "aws:ResourceAccount": "123456789012"
      }
    }
  ]
}

```

Amazon S3 on Outposts

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3-outposts:ListBucket",
        "s3-outposts:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/bucket/amzn-s3-demo-bucket",
        "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/accesspoint/bucket-access-point-name"
      ]
    },
    {
      "Action": [
        "s3-outposts:AbortMultipartUpload",
        "s3-outposts>DeleteObject",
        "s3-outposts:GetObject",
        "s3-outposts:GetObjectTagging",
        "s3-outposts:GetObjectVersion",
        "s3-outposts:GetObjectVersionTagging",
        "s3-outposts:ListMultipartUploadParts",
        "s3-outposts:PutObject",
        "s3-outposts:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/bucket/amzn-s3-demo-bucket/*",
        "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/accesspoint/bucket-access-point-name/*"
      ]
    }
  ]
}

```

```

    ]
  },
  {
    "Action": "s3-outposts:GetAccessPoint",
    "Effect": "Allow",
    "Resource": "arn:aws:s3-outposts:us-  
east-1:123456789012:outpost/outpost-id/accesspoint/bucket-access-point-name"
  }
]
}

```

Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort

Wenn [Sie Ihren Amazon S3 S3-Standort in der Konsole erstellen](#), DataSync können Sie automatisch eine IAM-Rolle erstellen und annehmen, die normalerweise über die richtigen Berechtigungen für den Zugriff auf Ihren S3-Bucket verfügt.

In einigen Situationen müssen Sie diese Rolle möglicherweise manuell erstellen (z. B. für den Zugriff auf Buckets mit zusätzlichen Sicherheitsebenen oder für die Übertragung zu oder von einem Bucket in einem anderen AWS-Konten).

Manuelles Erstellen einer IAM-Rolle für DataSync

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen und dann Rolle erstellen aus.
3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option AWS-Service.
4. Wählen Sie DataSync in der Dropdownliste für Anwendungsfall die Option aus und wählen Sie aus DataSync. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus. Geben Sie Ihrer Rolle einen Namen und wählen Sie Rolle erstellen.
6. Suchen Sie auf der Seite Rollen nach der Rolle, die Sie gerade erstellt haben, und wählen Sie ihren Namen aus.
7. Wählen Sie auf der Detailseite der Rolle den Tab Berechtigungen aus. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
8. Wählen Sie die Registerkarte JSON und [fügen Sie die für den Zugriff auf Ihren Bucket erforderlichen Berechtigungen](#) zum Richtlinieneditor hinzu.

9. Wählen Sie Weiter aus. Geben Sie Ihrer Richtlinie einen Namen und wählen Sie Richtlinie erstellen aus.
10. (Empfohlen) Gehen Sie wie folgt vor, um das [dienstübergreifende Problem mit verwirrten Stellvertretern](#) zu vermeiden:
 - a. Wählen Sie auf der Detailseite der Rolle die Registerkarte Vertrauensbeziehungen aus. Wählen Sie Vertrauensrichtlinie bearbeiten aus.
 - b. Aktualisieren Sie die Vertrauensrichtlinie anhand des folgenden Beispiels, das die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel enthält:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "444455556666"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:datasync:us-east-1:444455556666:*"
        }
      }
    }
  ]
}
```

- c. Wählen Sie Richtlinie aktualisieren.

Sie können diese Rolle bei der Erstellung Ihres Amazon S3 S3-Standorts angeben.

Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung

DataSync kann Daten zu oder von [S3-Buckets übertragen, die serverseitige Verschlüsselung verwenden](#). Die Art des Verschlüsselungsschlüssels, den ein Bucket verwendet, kann bestimmen, ob Sie eine benutzerdefinierte Richtlinie für den DataSync Zugriff auf den Bucket benötigen.

Beachten Sie bei der Verwendung DataSync mit S3-Buckets, die serverseitige Verschlüsselung verwenden, Folgendes:

- Wenn Ihr S3-Bucket mit einem AWS verwalteten Schlüssel verschlüsselt ist, DataSync können Sie standardmäßig auf die Objekte des Buckets zugreifen, wenn sich alle Ihre Ressourcen im selben Bucket befinden. AWS-Konto
- Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten AWS Key Management Service (AWS KMS) Schlüssel (SSE-KMS) verschlüsselt ist, muss die [Richtlinie des Schlüssels](#) die IAM-Rolle enthalten, die für den Zugriff auf den Bucket DataSync verwendet wird.
- Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten SSE-KMS-Schlüssel verschlüsselt ist und sich in einem anderen AWS-Konto befindet, ist eine Zugriffsberechtigung für den Bucket im anderen DataSync erforderlich. AWS-Konto Sie können dies wie folgt einrichten:
 - In der DataSync verwendeten IAM-Rolle müssen Sie den SSE-KMS-Schlüssel des kontoübergreifenden Buckets angeben, indem Sie den vollqualifizierten Amazon-Ressourcennamen (ARN) des Schlüssels verwenden. Dies ist derselbe Schlüssel-ARN, den Sie verwenden, um die [Standardverschlüsselung](#) des Buckets zu konfigurieren. In dieser Situation können Sie keine Schlüssel-ID, keinen Aliasnamen oder einen Alias-ARN angeben.

Hier ist ein Beispiel für einen Schlüssel-ARN:

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Weitere Informationen zur Angabe von KMS-Schlüsseln in IAM-Richtlinienerklärungen finden Sie im [AWS Key Management Service Entwicklerhandbuch](#).

- [Geben Sie in der SSE-KMS-Schlüsselrichtlinie die IAM-Rolle an, die](#) von verwendet wird. DataSync
- Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten AWS KMS Schlüssel (DSSE-KMS) für die serverseitige Dual-Layer-Verschlüsselung verschlüsselt ist, muss die [Richtlinie des Schlüssels](#) die IAM-Rolle enthalten, die für den Zugriff auf den Bucket verwendet wird. DataSync (Beachten Sie, dass DSSE-KMS keine [S3-Bucket-Keys](#) unterstützt, wodurch die Anforderungskosten gesenkt werden können.) AWS KMS

- Wenn Ihr S3-Bucket mit einem vom Kunden bereitgestellten Verschlüsselungsschlüssel (SSE-C) verschlüsselt ist, DataSync können Sie nicht auf diesen Bucket zugreifen.

Beispiel: SSE-KMS-Schlüsselrichtlinie für DataSync

Das folgende Beispiel ist eine [Schlüsselrichtlinie](#) für einen vom Kunden verwalteten SSE-KMS-Schlüssel. Die Richtlinie ist einem S3-Bucket zugeordnet, der serverseitige Verschlüsselung verwendet.

Wenn Sie dieses Beispiel verwenden möchten, ersetzen Sie die folgenden Werte durch Ihre eigenen:

- *account-id*— Ihr AWS-Konto.
- *admin-role-name*— Der Name der IAM-Rolle, die den Schlüssel verwalten kann.
- *datasync-role-name*— Der Name der IAM-Rolle, die es ermöglicht, den Schlüssel beim Zugriff auf den Bucket DataSync zu verwenden.

JSON

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
      "Resource": ""
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/admin-role-name"
      },
      "Action": [
        "kms:Create*",
        "kms:Describe*",
```

```

        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*",
        "kms:TagResource",
        "kms:UntagResource",
        "kms:ScheduleKeyDeletion",
        "kms:CancelKeyDeletion"
    ],
    "Resource": "*"
},
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/datasync-role-name"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
]
}

```

Zugriff auf eingeschränkte S3-Buckets

Wenn Sie zu oder von einem S3-Bucket wechseln müssen, der normalerweise jeglichen Zugriff verweigert, können Sie die Bucket-Richtlinie so bearbeiten, dass nur für Ihre Übertragung auf den Bucket zugegriffen werden DataSync kann.

Beispiel: Zulassen des Zugriffs auf der Grundlage von IAM-Rollen

1. Kopieren Sie die folgende S3-Bucket-Richtlinie.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "Deny-access-to-bucket",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "Condition": {
      "StringNotLike": {
        "aws:userid": [
          "datasync-iam-role-id:",
          "your-iam-role-id"
        ]
      }
    }
  }]
}
```

2. Ersetzen Sie in der Richtlinie die folgenden Werte:

- *amzn-s3-demo-bucket*— Geben Sie den Namen des eingeschränkten S3-Buckets an.
- *datasync-iam-role-id*— Geben Sie die ID der [IAM-Rolle an, die für den Zugriff auf den Bucket DataSync verwendet](#) wird.

Führen Sie den folgenden AWS CLI Befehl aus, um die IAM-Rollen-ID abzurufen:

```
aws iam get-role --role-name datasync-iam-role-name
```

Suchen Sie in der Ausgabe nach dem RoleId Wert:

```
"RoleId": "ANPAJ2UCCR6DPCEXAMPLE"
```

- *your-iam-role-id*— Geben Sie die ID der IAM-Rolle an, mit der Sie Ihren DataSync Standort für den Bucket erstellen.

Führen Sie den folgenden Befehl aus, um die IAM-Rollen-ID abzurufen:

```
aws iam get-role --role-name your-iam-role-name
```

Suchen Sie in der Ausgabe nach dem RoleId Wert:

```
"RoleId": "AIDACKCEVSQ6C2EXAMPLE"
```

3. [Fügen Sie diese Richtlinie](#) zu Ihrer S3-Bucket-Richtlinie hinzu.
4. Wenn Sie den eingeschränkten Bucket nicht mehr verwenden DataSync , entfernen Sie die Bedingungen für beide IAM-Rollen aus der Bucket-Richtlinie.

Zugriff auf S3-Buckets mit eingeschränktem VPC-Zugriff

Ein Amazon S3 S3-Bucket, der [den Zugriff auf bestimmte Virtual Private Cloud \(VPC\) -Endpunkte einschränkt oder VPCs](#) die Übertragung zu oder DataSync von diesem Bucket verweigert. Um Übertragungen in diesen Situationen zu ermöglichen, können Sie die Richtlinie des Buckets so aktualisieren, dass sie die IAM-Rolle enthält, die Sie [mit Ihrem Standort angeben](#). DataSync

Option 1: Allowing access based on DataSync location role ARN

In der S3-Bucket-Richtlinie können Sie den Amazon-Ressourcennamen (ARN) Ihrer DataSync Standort-IAM-Rolle angeben.

Das folgende Beispiel ist eine S3-Bucket-Richtlinie, die allen außer zwei VPCs (vpc-1234567890abcdef0 und vpc-abcdef01234567890) den Zugriff verweigert. Die Richtlinie umfasst jedoch auch den [ArnNotLikelyExists](#) Bedingungsschlüssel condition und [aws:PrincipalArn](#) condition, mit denen der ARN einer DataSync Standortrolle auf den Bucket zugreifen kann.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCs-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": [
```



```

        "vpc-1234567890abcdef0",
        "vpc-abcdef01234567890"
    ],
    },
    "ArnNotLikeIfExists": {
        "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/datasync-location-role-
name"
        ]
    }
}

```

Option 2: Allowing access based on DataSync location role tag

In der S3-Bucket-Richtlinie können Sie ein Tag angeben, das an Ihre DataSync Standort-IAM-Rolle angehängt ist.

Das folgende Beispiel ist eine S3-Bucket-Richtlinie, die allen außer zwei VPCs (vpc-1234567890abcdef0 und vpc-abcdef01234567890) den Zugriff verweigert. Die Richtlinie umfasst jedoch auch den [StringNotEqualsIfExists](#) Bedingungsschlüssel condition und [aws: PrincipalTag](#) condition, die einen Prinzipal mit dem Tag key exclude-from-vpc-restriction and value true zulassen. Sie können einen ähnlichen Ansatz in Ihrer Bucket-Richtlinie ausprobieren, indem Sie ein Tag angeben, das Ihrer DataSync Standortrolle zugeordnet ist.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCs-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": [
            "vpc-1234567890abcdef0",

```

```

        "vpc-abcdef01234567890"
      ],
      "aws:PrincipalTag/exclude-from-vpc-restriction": "true"
    }
  }
}
]
}

```

Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen

Wenn Amazon S3 Ihr Zielort ist, DataSync können Sie Ihre Daten direkt in eine bestimmte [Amazon S3 S3-Speicherklasse](#) übertragen.

Einige Speicherklassen weisen Verhaltensweisen auf, die sich auf Ihre Amazon S3 S3-Speicherkosten auswirken können. Wenn Sie Speicherklassen verwenden, für die zusätzliche Gebühren für das Überschreiben, Löschen oder Abrufen von Objekten anfallen können, führen Änderungen an Objektdaten oder Metadaten zu solchen Gebühren. Weitere Informationen finden Sie unter [Amazon S3 – Preise](#).

Important

Neue Objekte, die an Ihren Amazon S3 S3-Zielort übertragen werden, werden mit der Speicherklasse gespeichert, die Sie bei der [Erstellung Ihres Standorts](#) angeben. Standardmäßig wird die Speicherklasse vorhandener Objekte an Ihrem Zielort DataSync beibehalten, sofern Sie Ihre Aufgabe nicht so konfigurieren, dass [alle Daten übertragen](#) werden. In diesen Situationen wird die Speicherklasse, die Sie bei der Erstellung Ihres Standorts angeben, für alle Objekte verwendet.

Amazon S3 S3-Speicherklasse	Überlegungen
S3 Standard	Wählen Sie S3 Standard, um Ihre häufig aufgerufenen Dateien redundant in mehreren Availability Zones zu speichern, die geografisch getrennt sind. Dies ist die Standardeinstellung, wenn Sie keine Speicherklasse angeben.

Amazon S3 S3-Speicherkategorie	Überlegungen
S3 Intelligent-Tiering	Wählen Sie S3 Intelligent-Tiering, um die Speicherkosten zu optimieren, indem Sie Daten automatisch zur kostengünstigsten Speicherzugriffsstufe verschieben. Sie zahlen eine monatliche Gebühr pro Objekt, das in der Speicherkategorie S3 Intelligent-Tiering gespeichert ist. Diese Amazon S3 S3-Gebühr beinhaltet die Überwachung von Datenzugriffsmustern und das Verschieben von Objekten zwischen Stufen.
S3 Standard-IA	Wählen Sie S3 Standard-IA, um Ihre Objekte, auf die selten zugegriffen wird, redundant in mehreren Availability Zones zu speichern, die geografisch getrennt sind. Für Objekte, die in der Speicherkategorie S3 Standard-IA gespeichert sind, können zusätzliche Gebühren für das Überschreiben, Löschen oder Abrufen anfallen. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Änderungen an Objektdaten oder Metadaten entsprechen dem Löschen eines Objekts und dem Erstellen eines neuen Objekts, um es zu ersetzen. Dies führt zu zusätzlichen Gebühren für Objekte, die in der Speicherkategorie S3 Standard-IA gespeichert sind. Objekte mit weniger als 128 KB unterschreiten die Mindestkapazitätsgebühr pro Objekt in der Speicherkategorie S3 Standard-IA. Diese Objekte werden in der Speicherkategorie S3 Standard gespeichert.

Amazon S3 S3-Speicherkategorie	Überlegungen
S3 One Zone-IA	Wählen Sie S3 One Zone-IA, um Ihre selten aufgerufenen Objekte in einer einzigen Availability Zone zu speichern. Für Objekte, die in der Speicherkategorie S3 One Zone-IA gespeichert sind, können zusätzliche Gebühren für das Überschreiben, Löschen oder Abrufen anfallen. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Änderungen an Objektdaten oder Metadaten entsprechen dem Löschen eines Objekts und dem Erstellen eines neuen Objekts, um es zu ersetzen. Dies führt zu zusätzlichen Gebühren für Objekte, die in der Speicherkategorie S3 One Zone-IA gespeichert sind. Objekte mit weniger als 128 KB unterschreiten die Mindestkapazitätsgebühr pro Objekt in der Speicherkategorie S3 One Zone-IA. Diese Objekte werden in der Speicherkategorie S3 Standard gespeichert.

Amazon S3 S3-Speicherklassen	Überlegungen
S3 Glacier Instant Retrieval	Wählen Sie S3 Glacier Instant Retrieval, um Objekte zu archivieren, auf die selten zugegriffen wird, die aber innerhalb von Millisekunden abgerufen werden müssen. Daten, die in der Speicherklasse S3 Glacier Instant Retrieval gespeichert sind, bieten Kosteneinsparungen im Vergleich zur Speicherklasse S3 Standard-IA bei gleicher Latenz und Durchsatzleistung. S3 Glacier Instant Retrieval hat jedoch höhere Datenzugriffskosten als S3 Standard-IA. Für in S3 Glacier Instant Retrieval gespeicherte Objekte können zusätzliche Gebühren für das Überschreiben, Löschen oder Abrufen anfallen. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Änderungen an Objektdaten oder Metadaten entsprechen dem Löschen eines Objekts und dem Erstellen eines neuen Objekts, um es zu ersetzen. Dies führt zu zusätzlichen Gebühren für Objekte, die in der Speicherklasse S3 Glacier Instant Retrieval gespeichert sind. Objekte mit weniger als 128 KB unterschreiten die Mindestkapazitätsg Gebühr pro Objekt in der Speicherklasse S3 Glacier Instant Retrieval. Diese Objekte werden in der Speicherklasse S3 Standard gespeichert.

Amazon S3 S3-Speicherklassen	Überlegungen
S3 Glacier Flexible Retrieval	Wählen Sie S3 Glacier Flexible Retrieval für aktivere Archive. Bei Objekten, die in S3 Glacier Flexible Retrieval gespeichert sind, können zusätzliche Gebühren für das Überschreiben, Löschen oder Abrufen anfallen. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Änderungen an Objektdaten oder Metadaten entsprechen dem Löschen eines Objekts und dem Erstellen eines neuen Objekts, um es zu ersetzen. Dies führt zu zusätzlichen Gebühren für Objekte, die in der Speicherklasse S3 Glacier Flexible Retrieval gespeichert sind. Die Speicherklasse S3 Glacier Flexible Retrieval erfordert 40 KB an zusätzlichen Metadaten für jedes archivierte Objekt. DataSync platziert Objekte, die weniger als 40 KB groß sind, in die Speicherklasse S3 Standard. Sie müssen in dieser Speicherklasse archivierte Objekte wiederherstellen, bevor Sie sie lesen DataSync können. Weitere Informationen finden Sie unter Arbeiten mit archivierten Objekten im Amazon S3 S3-Benutzerhandbuch. Wenn Sie S3 Glacier Flexible Retrieval verwenden, wählen Sie die Option Nur übertragene Daten verifizieren, um die Prüfsummen der Daten und Metadaten am Ende der Übertragung zu vergleichen. Sie können die Option Alle Daten im Ziel verifizieren für diese Speicherklasse nicht verwenden, da dafür alle vorhandenen Objekte vom Ziel abgerufen werden müssen.

Amazon S3 S3-Speicherklasse	Überlegungen
S3 Glacier Deep Archive	Wählen Sie S3 Glacier Deep Archive, um Ihre Objekte für die langfristige Datenspeicherung und digitale Aufbewahrung zu archivieren, wobei ein- oder zweimal pro Jahr auf Daten zugegriffen wird. Bei Objekten, die in S3 Glacier Deep Archive gespeichert sind, können zusätzliche Gebühren für das Überschreiben, Löschen oder Abrufen anfallen. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Änderungen an Objektdaten oder Metadaten entsprechen dem Löschen eines Objekts und dem Erstellen eines neuen Objekts, um es zu ersetzen. Dies führt zu zusätzlichen Gebühren für Objekte, die in der Speicherklasse S3 Glacier Deep Archive gespeichert sind. Die Speicherklasse S3 Glacier Deep Archive benötigt 40 KB an zusätzlichen Metadaten für jedes archivierte Objekt. DataSync platziert Objekte, die weniger als 40 KB groß sind, in die Speicherklasse S3 Standard. Sie müssen in dieser Speicherklasse archivierte Objekte wiederherstellen, bevor Sie sie lesen DataSync können. Weitere Informationen finden Sie unter Arbeiten mit archivierten Objekten im Amazon S3 S3-Benutzerhandbuch. Wenn Sie S3 Glacier Deep Archive verwenden, wählen Sie die Aufgabenoption Nur übertragene Daten verifizieren, um Daten- und Metadaten-Prüfsummen am Ende der Übertragung zu vergleichen. Sie können die Option Alle Daten im Ziel verifizieren für diese Speicherklasse nicht verwenden, da dafür alle vorhandenen Objekte vom Ziel abgerufen werden müssen.
S3-Outposts	Die Speicherklasse für Amazon S3 auf Outposts.

Bewertung der Kosten für S3-Anfragen bei der Verwendung DataSync

Bei Amazon S3 S3-Standorten entstehen Ihnen Kosten im Zusammenhang mit S3-API-Anfragen von DataSync. In diesem Abschnitt erfahren Sie, wie diese Anfragen DataSync verwendet werden und wie sie sich auf Ihre [Amazon S3 S3-Kosten](#) auswirken können.

Themen

- [S3-Anfragen von DataSync](#)
- [Kostenüberlegungen](#)

S3-Anfragen von DataSync

In der folgenden Tabelle werden die S3-Anfragen beschrieben, die beim Kopieren von Daten an oder von einem Amazon S3 S3-Standort gestellt werden DataSync können.

S3-Anfrage	Wie DataSync benutzt es
ListObjectV2	DataSync stellt mindestens eine LIST Anfrage für jedes Objekt, das mit einem Schrägstrich (/) endet, um die Objekte aufzulisten, die mit diesem Präfix beginnen. Diese Anforderung wird während der Vorbereitungsphase einer Aufgabe aufgerufen.
HeadObject	DataSync stellt während der Vorbereitungs - und Überprüfungsphase einer Aufgabe HEAD Anfragen zum Abrufen von Objektmetadaten. Je nachdem, wie Sie die Integrität der übertragenen Daten überprüfen DataSync möchten, kann es mehrere HEAD Anfragen pro Objekt geben.
GetObject	DataSync stellt während der Übertragungsphase einer Aufgabe GET Anfragen zum Lesen von Daten aus einem Objekt. Für große Objekte kann es mehrere GET Anfragen geben.

S3-Anfrage	Wie DataSync benutzt es
GetObjectTagging	Wenn Sie Ihre Aufgabe so konfigurieren, dass sie Objekt-Tags kopiert , DataSync sendet diese GET Anfragen, um während der Vorbereitungs - und Übertragungsphase der Aufgabe nach Objekt-Tags zu suchen.
PutObject	DataSync stellt während der Übertragn ungsphase einer Aufgabe PUT Anfragen zur Erstellung von Objekten und Präfixen in einem S3-Ziel-Bucket. Da die mehrteilige Upload-Fu nktion von Amazon S3 DataSync verwendet wird, kann es mehrere PUT Anfragen für große Objekte geben. Um die Speicherkosten zu minimieren, empfehlen wir die Verwendung einer Lebenszykluskonfiguration , um unvollständige mehrteilige Uploads zu verhindern.
PutObjectTagging	Wenn Ihre Quellobjekte über Tags verfügen und Sie Ihre Aufgabe so konfigurieren, dass Objekt-Tags kopiert werden, DataSync stellt diese PUT Anfragen bei der Übertragung dieser Tags.
CopyObject	DataSync COPYfordert nur dann an, eine Kopie eines Objekts zu erstellen, wenn sich die Metadaten dieses Objekts ändern. Dies kann passieren, wenn Sie ursprünglich Daten mit einem anderen Dienst oder Tool, dessen Metadaten nicht übernommen wurden, in den S3-Bucket kopiert haben.

Kostenüberlegungen

DataSync stellt jedes Mal, wenn Sie Ihre Aufgabe ausführen, S3-Anfragen an S3-Buckets. Dies kann dazu führen, dass sich die Gebühren in bestimmten Situationen summieren. Beispiel:

- Sie übertragen häufig Objekte in oder aus einem S3-Bucket.
- Sie übertragen vielleicht nicht viele Daten, aber Ihr S3-Bucket enthält viele Objekte. In diesem Szenario können Sie immer noch hohe Gebühren feststellen, da DataSync S3-Anfragen für jedes Objekt des Buckets gestellt werden.
- Sie übertragen zwischen S3-Buckets, ebenso DataSync wie S3-Anfragen an die Quelle und das Ziel.

Beachten Sie Folgendes, um die damit verbundenen Kosten für S3-Anfragen zu DataSync minimieren:

Themen

- [Welche S3-Speicherklassen verwende ich?](#)
- [Wie oft muss ich meine Daten übertragen?](#)

Welche S3-Speicherklassen verwende ich?

Die Gebühren für S3-Anfragen können je nach der Amazon S3 S3-Speicherklasse, die Ihre Objekte verwenden, variieren, insbesondere für Klassen, die Objekte archivieren (wie S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval und S3 Glacier Deep Archive).

Im Folgenden sind einige Szenarien aufgeführt, in denen sich Speicherklassen auf Ihre Gebühren für S3-Anfragen auswirken können, wenn Sie sie verwenden: DataSync

- Stellt jedes Mal, wenn Sie eine Aufgabe ausführen, DataSync HEAD Anfragen zum Abrufen von Objektmetadaten. Diese Anfragen führen zu Gebühren, auch wenn Sie keine Objekte verschieben. Wie stark sich diese Anfragen auf Ihre Rechnung auswirken, hängt von der Speicherklasse ab, die Ihre Objekte verwenden, und von der Anzahl der Objekte, die DataSync gescannt werden.
- Wenn Sie Objekte in die Speicherklasse S3 Glacier Instant Retrieval verschoben haben (entweder direkt oder über eine Bucket-Lebenszykluskonfiguration), sind Anfragen für Objekte dieser Klasse teurer als Objekte in anderen Speicherklassen.
- Wenn Sie Ihre DataSync Aufgabe so konfigurieren, [dass überprüft wird, ob Ihre Quell- und Zielspeicherorte vollständig synchronisiert sind](#), werden GET Anfragen für jedes Objekt in allen Speicherklassen (außer S3 Glacier Flexible Retrieval und S3 Glacier Deep Archive) gestellt.
- Zusätzlich zu GET Anfragen fallen für Sie Kosten für den Datenabruf für Objekte der Speicherklasse S3 Standard-IA, S3 One Zone-IA oder S3 Glacier Instant Retrieval an.

Weitere Informationen finden Sie unter [Amazon S3 – Preise](#).

Wie oft muss ich meine Daten übertragen?

Wenn Sie Daten regelmäßig verschieben müssen, sollten Sie sich einen [Zeitplan](#) überlegen, in dem nicht mehr Aufgaben ausgeführt werden, als Sie benötigen.

Sie können auch erwägen, den Umfang Ihrer Übertragungen einzuschränken. Sie können beispielsweise so konfigurieren, dass der Fokus DataSync auf Objekte in bestimmten Präfixen liegt, oder Sie können [filtern, welche Daten übertragen werden](#). Diese Optionen können dazu beitragen, die Anzahl der S3-Anfragen zu reduzieren, die bei jeder Ausführung Ihrer DataSync Aufgabe gestellt werden.

Überlegungen zu Objekten bei Amazon S3 S3-Übertragungen

- Wenn Sie Daten aus einem S3-Bucket übertragen, verwenden Sie [S3 Storage Lens](#), um zu ermitteln, wie viele Objekte Sie verschieben.
- Bei der Übertragung zwischen S3-Buckets empfehlen wir, den [erweiterten Aufgabenmodus](#) zu verwenden, da für Sie keine DataSync [Aufgabenkontingente](#) gelten.
- DataSync überträgt möglicherweise kein Objekt mit Sonderzeichen im Namen. Weitere Informationen finden Sie in den [Richtlinien zur Benennung von Objektschlüsseln](#) im Amazon S3 S3-Benutzerhandbuch.
- Beachten Sie bei der Verwendung DataSync mit einem S3-Bucket, der [Versionierung](#) verwendet, Folgendes:
 - DataSync Erstellt bei der Übertragung in einen S3-Bucket eine neue Version eines Objekts, wenn dieses Objekt an der Quelle geändert wird. Dies führt zu zusätzlichen Gebühren.
 - Ein Objekt hat unterschiedliche Versionen IDs im Quell- und Ziel-Bucket.
 - Nur die neueste Version jedes Objekts wird aus dem Quell-Bucket übertragen. Frühere Versionen werden nicht in das Ziel kopiert.
- Nach der anfänglichen Übertragung von Daten aus einem S3-Bucket in ein Dateisystem (z. B. NFS oder Amazon FSx) enthalten nachfolgende Ausführungen derselben DataSync Aufgabe keine Objekte, die geändert wurden, aber dieselbe Größe wie bei der ersten Übertragung haben.

Ihren Übertragungsort für einen Amazon S3 S3-Allzweck-Bucket erstellen

Um einen Standort für Ihre Übertragung zu erstellen, benötigen Sie einen vorhandenen S3-Allzweck-Bucket. Falls Sie noch keinen haben, finden Sie weitere Informationen im [Amazon S3 S3-Benutzerhandbuch](#).

Important

Bevor Sie Ihren Standort erstellen, stellen Sie sicher, dass Sie die folgenden Abschnitte gelesen haben:

- [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#)
- [Bewertung der Kosten für S3-Anfragen bei der Verwendung DataSync](#)

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp Amazon S3 und dann General Purpose Bucket aus.
4. Geben Sie für S3-URI den Bucket und das Präfix ein, das Sie für Ihren Standort verwenden möchten, oder wählen Sie es aus.

Warning

DataSync kann keine Objekte mit einem Präfix übertragen, das mit einem Schrägstrich (/) beginnt oder /. . / Muster enthält//. . / Beispiel:

- `/photos`
- `photos//2006/January`
- `photos/. /2006/February`
- `photos/. . /2006/March`

5. Wählen Sie für S3-Speicherklasse bei Verwendung als Ziel eine Speicherklasse aus, die Ihre Objekte verwenden sollen, wenn Amazon S3 ein Übertragungsziel ist.

Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#).

6. Führen Sie für IAM role (IAM-Rolle) einen der folgenden Schritte aus:

- Wählen Sie Automatisch generieren für DataSync , um automatisch eine IAM-Rolle mit den für den Zugriff auf den S3-Bucket erforderlichen Berechtigungen zu erstellen.

Wenn Sie DataSync zuvor eine IAM-Rolle für diesen S3-Bucket erstellt haben, wird diese Rolle standardmäßig ausgewählt.

- Wählen Sie eine benutzerdefinierte IAM-Rolle aus, die Sie erstellt haben. Weitere Informationen finden Sie unter [Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort](#).

7. (Optional) Wählen Sie Neues Tag hinzufügen, um Ihren Amazon S3 S3-Standort zu kennzeichnen.

Mithilfe von Tags können Sie Ihre Ressourcen verwalten, filtern und suchen. Wir empfehlen, ein Namensschild für Ihren Standort zu erstellen.

8. Wählen Sie Standort erstellen.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden create-location-s3 Befehl:

```
aws datasync create-location-s3 \
  --s3-bucket-arn 'arn:aws:s3:::amzn-s3-demo-bucket' \
  --s3-storage-class 'your-S3-storage-class' \
  --s3-config 'BucketAccessRoleArn=arn:aws:iam::account-id:role/role-allowing-  
datasync-operations' \
  --subdirectory /your-prefix-name
```

2. Geben Sie für --s3-bucket-arn den ARN des S3-Buckets an, den Sie als Speicherort verwenden möchten.
3. Geben Sie für --s3-storage-class eine Speicherklasse an, die Ihre Objekte verwenden sollen, wenn Amazon S3 ein Übertragungsziel ist.
4. Geben Sie für --s3-config den ARN der IAM-Rolle an, die auf Ihren Bucket zugreifen DataSync muss.

Weitere Informationen finden Sie unter [Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort](#).

5. Geben Sie für `--subdirectory` ein Präfix im S3-Bucket an, aus dem DataSync gelesen oder geschrieben wird (je nachdem, ob es sich bei dem Bucket um einen Quell- oder Zielspeicherort handelt).

 Warning

DataSync kann keine Objekte mit einem Präfix übertragen, das mit einem Schrägstrich (/) beginnt oder /. ./ Muster einschließt//. ./ Beispiel:

- /photos
- photos//2006/January
- photos/./2006/February
- photos/./2006/March

6. Führen Sie den Befehl `create-location-s3` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN des Speicherorts anzeigt, den Sie erstellt haben. Beispiel:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Sie können diesen Speicherort als Quelle oder Ziel für Ihre DataSync Aufgabe verwenden.

Erstellen Sie Ihren Transferort für einen S3-Bucket auf Outposts

Um einen Standort für Ihre Übertragung zu erstellen, benötigen Sie einen vorhandenen Amazon S3 on Outposts-Bucket. Falls Sie noch keinen haben, finden Sie weitere Informationen im [Amazon S3 on Outposts-Benutzerhandbuch](#).

Sie benötigen auch einen DataSync Agenten. Weitere Informationen finden Sie unter [Bereitstellen Ihres Agenten im Basismodus auf AWS Outposts](#).

Bei der Übertragung von einem S3-Bucket-Präfix auf Outposts, das einen großen Datensatz enthält (z. B. Hunderttausende oder Millionen von Objekten), kann es zu einem Timeout für Ihre DataSync Aufgabe kommen. Um dies zu vermeiden, sollten Sie ein [DataSync Manifest](#) verwenden, mit dem Sie genau die Objekte angeben können, die Sie übertragen müssen.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp Amazon S3 und dann Outposts Bucket aus.
4. Wählen Sie für den S3-Bucket einen Amazon S3 S3-Zugriffspunkt, der auf Ihren S3 on Outposts-Bucket zugreifen kann.

Weitere Informationen finden Sie im [Amazon S3 S3-Benutzerhandbuch](#).

5. Wählen Sie für S3-Speicherklasse bei Verwendung als Ziel eine Speicherklasse aus, die Ihre Objekte verwenden sollen, wenn Amazon S3 ein Übertragungsziel ist.

Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#). DataSync verwendet standardmäßig die Speicherklasse S3 Outposts für Amazon S3 auf Outposts.

6. Geben Sie für Agenten den Amazon-Ressourcennamen (ARN) des DataSync Agenten in Ihrem Outpost an.
7. Geben Sie für Ordner ein Präfix im S3-Bucket ein, das aus oder DataSync in das geschrieben wird (je nachdem, ob es sich bei dem Bucket um einen Quell- oder Zielspeicherort handelt).

Warning

DataSync kann keine Objekte mit einem Präfix übertragen, das mit einem Schrägstrich (/) beginnt oder /. / Muster einschließt/. / . / Beispiel:

- /photos
- photos//2006/January
- photos/. /2006/February
- photos/. /. /2006/March

8. Führen Sie für IAM role (IAM-Rolle) einen der folgenden Schritte aus:

- Wählen Sie Automatisch generieren für DataSync , um automatisch eine IAM-Rolle mit den für den Zugriff auf den S3-Bucket erforderlichen Berechtigungen zu erstellen.

Wenn Sie DataSync zuvor eine IAM-Rolle für diesen S3-Bucket erstellt haben, wird diese Rolle standardmäßig ausgewählt.

- Wählen Sie eine benutzerdefinierte IAM-Rolle aus, die Sie erstellt haben. Weitere Informationen finden Sie unter [Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort](#).

9. (Optional) Wählen Sie Neues Tag hinzufügen, um Ihren Amazon S3 S3-Standort zu kennzeichnen.

Mithilfe von Tags können Sie Ihre Ressourcen verwalten, filtern und suchen. Wir empfehlen, ein Namensschild für Ihren Standort zu erstellen.

10. Wählen Sie Standort erstellen.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden create-location-s3 Befehl:

```
aws datasync create-location-s3 \
  --s3-bucket-arn 'bucket-access-point' \
  --s3-storage-class 'your-S3-storage-class' \
  --s3-config 'BucketAccessRoleArn=arn:aws:iam::account-id:role/role-allowing-  
datasync-operations' \
  --subdirectory /your-folder \
  --agent-arns 'arn:aws:datasync:your-region:account-id:agent/agent-agent-id'
```

2. Geben Sie für --s3-bucket-arn den ARN einen Amazon S3 S3-Zugriffspunkt an, der auf Ihren S3 on Outposts-Bucket zugreifen kann.

Weitere Informationen finden Sie im [Amazon S3 S3-Benutzerhandbuch](#).

3. Geben Sie für --s3-storage-class eine Speicherklasse an, die Ihre Objekte verwenden sollen, wenn Amazon S3 ein Übertragungsziel ist.

Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#). DataSync verwendet standardmäßig die Speicherklasse S3 Outposts für S3 auf Outposts.

4. Geben Sie für `--s3-config` den ARN der IAM-Rolle an, die auf Ihren Bucket zugreifen DataSync muss.

Weitere Informationen finden Sie unter [Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort](#).

5. Geben Sie für `--subdirectory` ein Präfix im S3-Bucket an, aus dem DataSync gelesen oder geschrieben wird (je nachdem, ob es sich bei dem Bucket um einen Quell- oder Zielspeicherort handelt).

 Warning

DataSync kann keine Objekte mit einem Präfix übertragen, das mit einem Schrägstrich (/) beginnt oder /. ./ Muster einschließt//. ./ Beispiel:

- /photos
- photos//2006/January
- photos/. ./2006/February
- photos/. ./2006/March

6. Geben Sie für `--agent-arns` den ARN des DataSync Agenten in Ihrem Outpost an.
7. Führen Sie den Befehl `create-location-s3` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN des Speicherorts anzeigt, den Sie erstellt haben. Beispiel:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Sie können diesen Speicherort als Quelle oder Ziel für Ihre DataSync Aufgabe verwenden.

Amazon S3 S3-Übertragungen zwischen AWS-Konten

Mit DataSync können Sie Daten in [verschiedene AWS-Konten](#) S3-Buckets verschieben. Weitere Informationen finden Sie in den folgenden Tutorials:

- [Übertragung von Daten aus dem lokalen Speicher zu Amazon S3 über AWS-Konten](#)

- [Übertragung von Daten von Amazon S3 zu Amazon S3 über AWS-Konten](#)

Amazon S3 S3-Übertragungen zwischen kommerziellen und AWS GovCloud (US) Regions

Standardmäßig werden DataSync keine Übertragungen zwischen S3-Buckets im kommerziellen und AWS GovCloud (US) Regions. Sie können diese Art der Übertragung jedoch trotzdem einrichten, indem Sie einen Objektspeicherort für einen der S3-Buckets in Ihrer Übertragung erstellen. Sie können diese Art der Übertragung mit oder ohne Agenten durchführen. Wenn Sie einen Agenten verwenden, muss Ihre Aufgabe für den Basismodus konfiguriert sein. Um ohne Agenten zu übertragen, müssen Sie den erweiterten Modus verwenden.

Bevor Sie beginnen: Vergewissern Sie sich, dass Sie die Kosten verstehen, die eine Übertragung zwischen Regionen mit sich bringt. Weitere Informationen finden Sie unter [AWS DataSync – Preise](#).

Inhalt

- [Bereitstellung des DataSync Zugriffs auf den Bucket Ihres Objektspeichers](#)
- [Erstellen Sie Ihren DataSync Agenten \(optional\)](#)
- [Einen Objektspeicherort für Ihren S3-Bucket erstellen](#)

Bereitstellung des DataSync Zugriffs auf den Bucket Ihres Objektspeichers

Wenn Sie den Objektspeicherort für diese Übertragung erstellen, müssen Sie DataSync die Anmeldeinformationen eines IAM-Benutzers angeben, der berechtigt ist, auf den S3-Bucket des Standorts zuzugreifen. Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

Warning

IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

Erstellen Sie Ihren DataSync Agenten (optional)

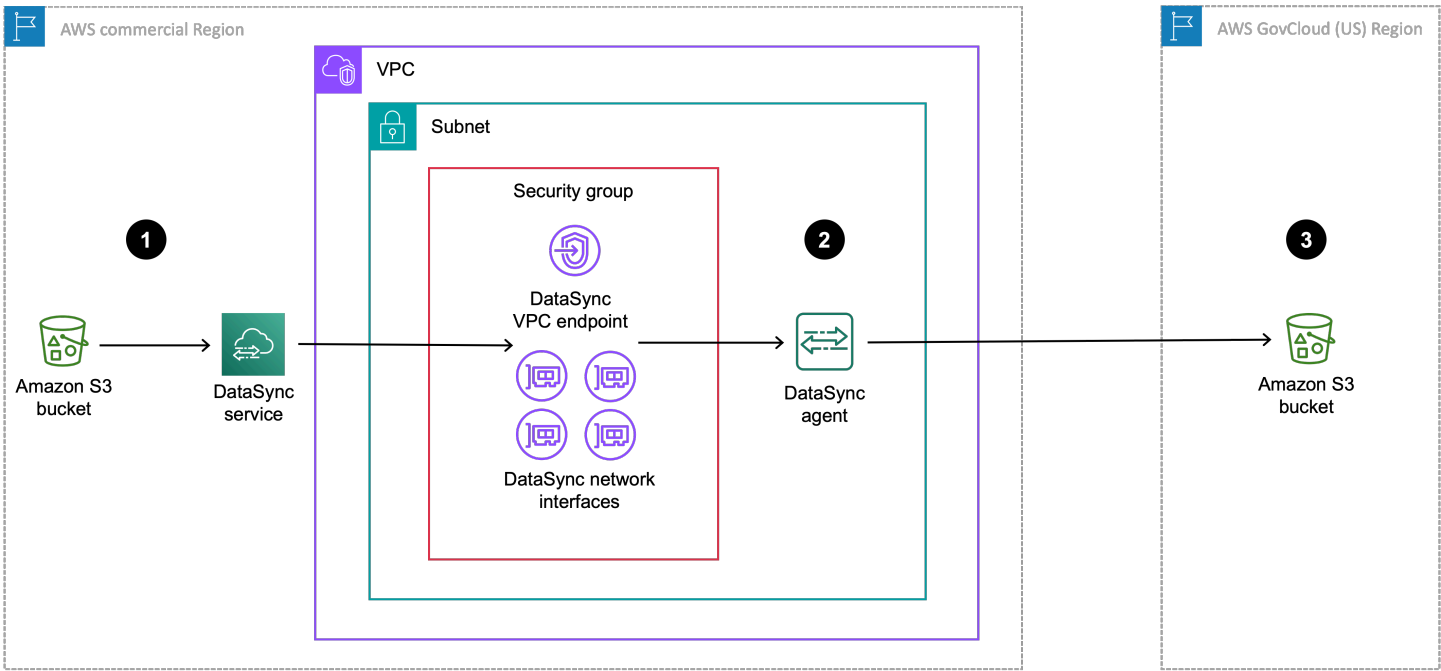
Wenn Sie Ihre Übertragung im Basismodus ausführen möchten, müssen Sie einen Agenten verwenden. Da Sie zwischen einer kommerziellen und einer anderen wechseln AWS GovCloud

(US) Region, setzen Sie Ihren DataSync Agenten als EC2 Amazon-Instance in einer der Regionen ein. Wir empfehlen, dass Ihr Agent einen VPC-Serviceendpoint verwendet, um Gebühren für die Datenübertragung ins öffentliche Internet zu vermeiden. Weitere Informationen finden Sie unter [Amazon EC2 Data Transfer — Preise](#).

Wählen Sie eines der folgenden Szenarien, in denen beschrieben wird, wie Sie einen Agenten erstellen, der auf der Region basiert, in der Sie Ihre DataSync Aufgabe ausführen möchten.

Wenn Sie eine DataSync Aufgabe in einer Handelsregion ausführen

Das folgende Diagramm zeigt eine Übertragung, bei der sich Ihre DataSync Aufgabe und Ihr Agent in der Handelsregion befinden.



Referenz	Description
1	In der kommerziellen Region, in der Sie eine DataSync Aufgabe ausführen, werden Daten aus dem S3-Quell-Bucket übertragen. Der Quell-Bucket ist als Amazon S3 S3-Standort in der Handelsregion konfiguriert.
2	Datenübertragungen über den DataSync Agenten, der sich in derselben VPC und demselben Subnetz befindet, in denen sich der VPC-Dienstendpunkt und die Netzwerkschnittstellen befinden .

Referenz	Description
3	Datenübertragungen an den Ziel-S3-Bucket im. AWS GovCloud (US) Region Der Ziel-Bucket ist als Objektspeicherort in der Handelsregion konfiguriert.

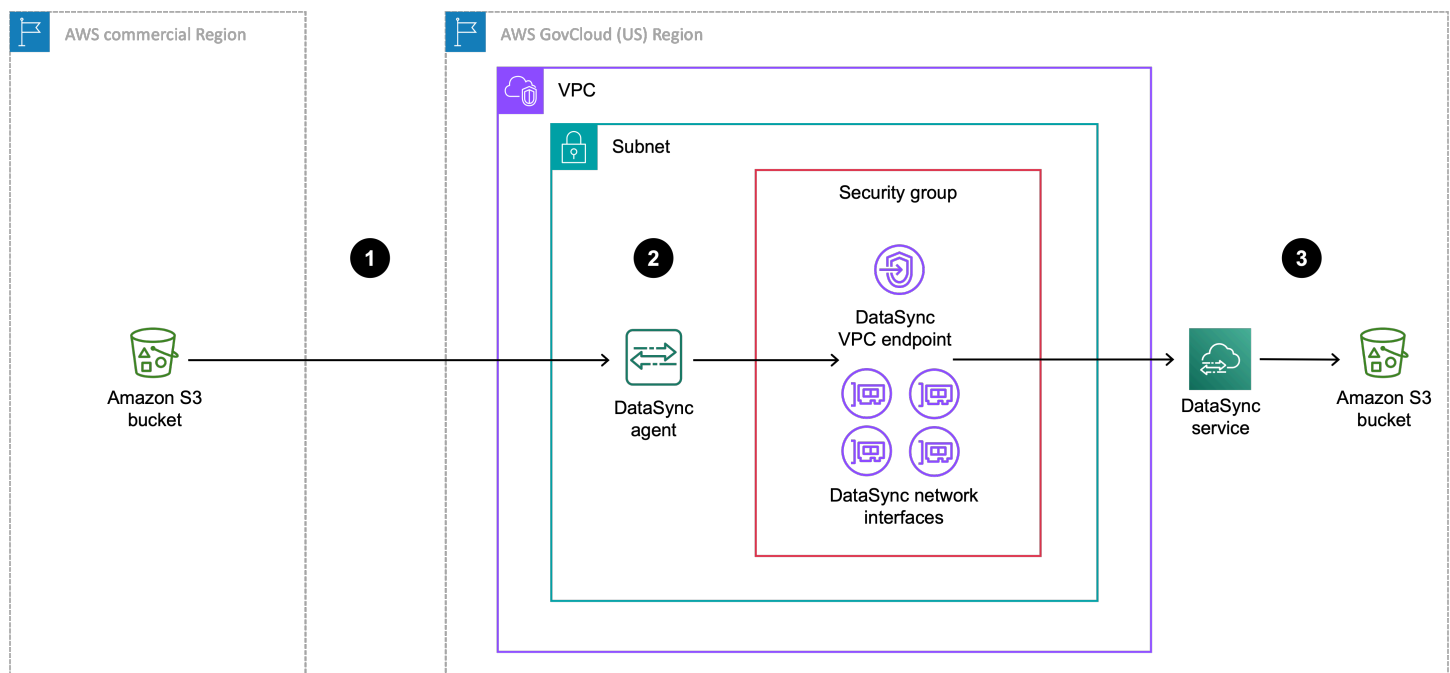
Sie können dasselbe Setup verwenden, um auch die umgekehrte Richtung von der Handelsregion in die Handelsregion AWS GovCloud (US) Region zu übertragen.

Um Ihren DataSync Agenten zu erstellen

1. [Stellen Sie einen EC2 Amazon-Agenten](#) in Ihrer Handelsregion bereit.
2. Konfigurieren Sie Ihren Agenten für die Verwendung eines [VPC-Serviceendpunkts](#).
3. [Aktivieren Sie Ihren Agenten](#).

Wenn Sie eine DataSync Aufgabe in einer Region GovCloud (USA) ausführen

Das folgende Diagramm zeigt eine Übertragung, bei der sich Ihre DataSync Aufgabe und Ihr Agent in der AWS GovCloud (US) Region.



Referenz	Description
1	Datenübertragungen vom S3-Quell-Bucket in der Handelsregion zu dem AWS GovCloud (US) Region Ort, an dem Sie eine DataSync Aufgabe ausführen. Der Quell-Bucket ist als Objektspeicherort im konfiguriert AWS GovCloud (US) Region.
2	In der AWS GovCloud (US) Region, Datenübertragungen über den DataSync Agenten in derselben VPC und demselben Subnetz, in dem sich der VPC-Dienstendpunkt und die Netzwerkschnittstellen befinden .
3	Datenübertragungen an den Ziel-S3-Bucket im. AWS GovCloud (US) Region Der Ziel-Bucket ist als Amazon S3 S3-Standort in der konfiguriert AWS GovCloud (US) Region.

Sie können dasselbe Setup verwenden, um auch die umgekehrte Richtung von der AWS GovCloud (US) Region zur Handelsregion zu übertragen.

Um Ihren DataSync Agenten zu erstellen

1. [Stellen Sie einen EC2 Amazon-Agenten](#) in Ihrem bereit AWS GovCloud (US) Region.
2. Konfigurieren Sie Ihren Agenten für die Verwendung eines [VPC-Serviceendpunkts](#).
3. [Aktivieren Sie Ihren Agenten](#).

Wenn Ihr Datensatz stark komprimierbar ist, können Sie die Kosten senken, wenn Sie Ihren Agenten stattdessen in einer Handelsregion erstellen und gleichzeitig eine Aufgabe in einer ausführen. AWS GovCloud (US) Region Die Erstellung dieses Agenten erfordert mehr Einstellungen als üblich, einschließlich der Vorbereitung des Agenten für den Einsatz in einer Handelsregion. Informationen zum Erstellen eines Agenten für dieses Setup finden Sie [im AWS DataSync Blog Daten ein- und AWS GovCloud \(US\) auslagern](#).

Einen Objektspeicherort für Ihren S3-Bucket erstellen

Sie benötigen einen Objektspeicherort für den S3-Bucket, der sich in der Region befindet, in der Sie Ihre DataSync Aufgabe nicht ausführen.

Verwenden der DataSync -Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Stellen Sie sicher, dass Sie sich in derselben Region befinden, in der Sie Ihre Aufgabe ausführen möchten.
3. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
4. Wählen Sie als Standorttyp die Option Objektspeicher aus.
5. Wählen Sie für Agenten den DataSync Agenten aus, den Sie für diese Übertragung erstellt haben.
6. Geben Sie für Server einen Amazon S3 S3-Endpunkt für Ihren Bucket ein, indem Sie eines der folgenden Formate verwenden:
 - Bucket für die Handelsregion: `s3.your-region.amazonaws.com`
 - AWS GovCloud (US) Region Eimer: `s3.your-gov-region.amazonaws.com`

Eine Liste der Amazon S3 S3-Endpunkte finden Sie unter [Allgemeine AWS-Referenz](#).

7. Geben Sie als Bucket-Namen den Namen des S3-Buckets ein.
8. Geben Sie für Ordner ein Präfix im S3-Bucket ein, das aus oder DataSync in das geschrieben wird (je nachdem, ob es sich bei dem Bucket um einen Quell- oder Zielspeicherort handelt).

Warning

DataSync kann keine Objekte mit einem Präfix übertragen, das mit einem Schrägstrich (/) beginnt oder /. ./ Muster einschließt/. ./ Beispiel:

- /photos
- photos//2006/January
- photos./2006/February
- photos../2006/March

9. Wählen Sie Anmeldedaten erforderlich aus und gehen Sie wie folgt vor:
 - Geben Sie unter Zugriffsschlüssel den Zugriffsschlüssel für einen [IAM-Benutzer](#) ein, der auf den Bucket zugreifen kann.

- Geben Sie unter Geheimer Schlüssel den geheimen Schlüssel desselben IAM-Benutzers ein.
10. (Optional) Wählen Sie Tag hinzufügen, um Ihren Standort zu taggen.

Mithilfe von Tags können Sie Ihre Ressourcen verwalten, filtern und suchen. Wir empfehlen, ein Namensschild für Ihren Standort zu erstellen.
 11. Wählen Sie Standort erstellen aus.

Verwendung der AWS CLI

1. Kopieren Sie den folgenden `create-location-object-storage` Befehl:

```
aws datasync create-location-object-storage \
  --server-hostname s3-endpoint \
  --bucket-name amzn-s3-demo-bucket \
  --agent-arns arn:aws:datasync:your-region:123456789012:agent/
agent-01234567890deadfb
```

2. Geben Sie für den `--server-hostname` Parameter einen Amazon S3 S3-Endpunkt für Ihren Bucket an, indem Sie eines der folgenden Formate verwenden:
 - Bucket für die Handelsregion: `s3.your-region.amazonaws.com`
 - AWS GovCloud (US) Region Eimer: `s3.your-gov-region.amazonaws.com`

Stellen Sie sicher, dass Sie für die Region auf dem Endpunkt dieselbe Region angeben, in der Sie Ihre Aufgabe ausführen möchten.

Eine Liste der Amazon S3 S3-Endpunkte finden Sie unter [Allgemeine AWS-Referenz](#).

3. Geben Sie für den `--bucket-name` Parameter den Namen des S3-Buckets an.
4. Geben Sie für den `--agent-arns` Parameter den DataSync Agenten an, den Sie für diese Übertragung erstellt haben.
5. Geben Sie für den `--access-key` Parameter den Zugriffsschlüssel für einen [IAM-Benutzer](#) an, der auf den Bucket zugreifen kann.
6. Geben Sie für den `--secret-key` Parameter den geheimen Schlüssel desselben IAM-Benutzers ein.

7. (Optional) Geben Sie für den `--subdirectory` Parameter ein Präfix im S3-Bucket an, das DataSync Lese- oder Schreibvorgänge vornimmt (je nachdem, ob es sich bei dem Bucket um einen Quell- oder Zielspeicherort handelt).

 Warning

DataSync kann keine Objekte übertragen, deren Präfix mit einem Schrägstrich (/) beginnt oder ein Include- `///./`, oder `/./` Muster enthält. Beispiel:

- `/photos`
- `photos//2006/January`
- `photos/./2006/February`
- `photos/./2006/March`

8. (Optional) Geben Sie für den `--tags` Parameter Schlüssel-Wert-Paare an, die Tags für die Standortressource darstellen.

Mithilfe von Tags können Sie Ihre Ressourcen verwalten, filtern und suchen. Wir empfehlen, ein Namensschild für Ihren Standort zu erstellen.

9. Führen Sie den Befehl `create-location-object-storage` aus.

Sie erhalten eine Antwort, die Ihnen den Standort-ARN anzeigt, den Sie gerade erstellt haben.

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-01234567890abcdef"
}
```

Sie können diesen Speicherort als Quelle oder Ziel für Ihre DataSync Aufgabe verwenden. [Erstellen Sie für den anderen S3-Bucket in dieser Übertragung einen Amazon S3 S3-Standort.](#)

Nächste Schritte

Zu den möglichen nächsten Schritten gehören:

1. Erstellen Sie bei Bedarf Ihren anderen Standort. Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

2. [Konfigurieren Sie unter anderem DataSync Aufgabeneinstellungen](#), z. B. welche Dateien übertragen werden sollen, wie mit Metadaten umgegangen werden soll.
3. [Legen Sie einen Zeitplan](#) für Ihre DataSync Aufgabe fest.
4. [Konfigurieren Sie die Überwachung](#) für Ihre DataSync Aufgabe.
5. [Starten](#) Sie Ihre Aufgabe.

Konfiguration von AWS DataSync Übertragungen mit Amazon EFS

Um Daten zu oder von Ihrem Amazon EFS-Dateisystem zu übertragen, müssen Sie einen AWS DataSync Übertragungsort erstellen. DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bereitstellung des DataSync Zugriffs auf Amazon EFS-Dateisysteme

[Um einen Standort zu erstellen](#), müssen Sie wissen, wie Sie auf Ihren Speicher zugreifen DataSync können. Mounten Sie für Amazon DataSync EFS Ihr Dateisystem als Root-Benutzer aus Ihrer Virtual Private Cloud (VPC) mithilfe von [Netzwerkschnittstellen](#).

Inhalt

- [Ermitteln des Subnetzes und der Sicherheitsgruppen für Ihr Mount-Ziel](#)
- [Zugriff auf eingeschränkte Dateisysteme](#)
 - [Eine DataSync IAM-Rolle für den Dateisystemzugriff erstellen](#)
 - [Beispiel für eine Dateisystemrichtlinie, die DataSync den Zugriff ermöglicht](#)

Ermitteln des Subnetzes und der Sicherheitsgruppen für Ihr Mount-Ziel

Bei der Erstellung Ihres Standorts geben Sie das Subnetz und die Sicherheitsgruppen an, die eine Verbindung DataSync zu einem der [Mount-Ziele](#) Ihres Amazon EFS-Dateisystems ermöglichen.

Das von Ihnen angegebene Subnetz muss sich befinden:

- In derselben VPC wie Ihr Dateisystem.
- In derselben Availability Zone wie mindestens ein Mount-Ziel für Ihr Dateisystem.

 Note

Sie müssen kein Subnetz angeben, das ein Bereitstellungsziel für das Dateisystem enthält.

Die von Ihnen angegebenen Sicherheitsgruppen müssen eingehenden Datenverkehr auf Port 2049 (Network File System) zulassen. Informationen zum Erstellen und Aktualisieren von Sicherheitsgruppen für Ihre Mount-Ziele finden Sie im [Amazon EFS-Benutzerhandbuch](#).

Angeben von Sicherheitsgruppen, die einem Mount-Ziel zugeordnet sind

Sie können eine Sicherheitsgruppe angeben, die einem der Mount-Ziele Ihres Dateisystems zugeordnet ist. Wir empfehlen diesen Ansatz aus Sicht der Netzwerkverwaltung.

Angabe von Sicherheitsgruppen, die keinem Mount-Ziel zugeordnet sind

Sie können auch eine Sicherheitsgruppe angeben, die keinem der Mount-Ziele Ihres Dateisystems zugeordnet ist. Diese Sicherheitsgruppe muss jedoch in der Lage sein, mit der Sicherheitsgruppe eines Mount-Ziels zu kommunizieren.

So könnten Sie beispielsweise eine Beziehung zwischen Sicherheitsgruppe D (für DataSync) und Sicherheitsgruppe M (für das Mount-Ziel) erstellen:

- Sicherheitsgruppe D, die Sie bei der Erstellung Ihres Standorts angeben, muss über eine Regel verfügen, die ausgehende Verbindungen über den NFS-Port 2049 zur Sicherheitsgruppe M zulässt.
- Die Sicherheitsgruppe M, die Sie dem Mount-Ziel zuordnen, muss eingehenden Zugriff auf den NFS-Port 2049 von der Sicherheitsgruppe D aus zulassen.

Um die Sicherheitsgruppe eines Mount-Ziels zu finden

Die folgenden Anweisungen können Ihnen helfen, die Sicherheitsgruppe eines Amazon EFS-Dateisystem-Mount-Ziels DataSync zu identifizieren, das Sie für Ihre Übertragung verwenden möchten.

1. Führen Sie im AWS CLI den folgenden `describe-mount-targets` Befehl aus.

```
aws efs describe-mount-targets \  
  --region file-system-region \  
  --file-system-id file-system-id
```

Dieser Befehl gibt Informationen über die Mount-Ziele Ihres Dateisystems zurück (ähnlich der folgenden Beispielausgabe).

```
{
  "MountTargets": [
    {
      "OwnerId": "111222333444",
      "MountTargetId": "fsmt-22334a10",
      "FileSystemId": "fs-123456ab",
      "SubnetId": "subnet-f12a0e34",
      "LifecycleState": "available",
      "IpAddress": "11.222.0.123",
      "NetworkInterfaceId": "eni-1234a044"
    }
  ]
}
```

2. Notieren Sie sich den MountTargetId Wert, den Sie verwenden möchten.
3. Führen Sie den folgenden describe-mount-target-security-groups Befehl mit dem ausMountTargetId, um die Sicherheitsgruppe Ihres Mount-Ziels zu sehen.

```
aws efs describe-mount-target-security-groups \
  --region file-system-region \
  --mount-target-id mount-target-id
```

Sie geben diese Sicherheitsgruppe an, wenn [Sie Ihren Standort erstellen](#).

Zugriff auf eingeschränkte Dateisysteme

DataSync kann Daten zu oder von Amazon EFS-Dateisystemen übertragen, die den Zugriff über [Zugriffspunkte](#) und [IAM-Richtlinien](#) einschränken.

Note

Wenn DataSync auf ein Zieldateisystem über einen Zugriffspunkt zugegriffen wird, der die Benutzeridentität erzwingt, bleiben der POSIX-Benutzer und die POSIX-Gruppe IDs für Ihre Quelldaten nicht erhalten, wenn Sie Ihre DataSync Aufgabe so konfigurieren, dass der Besitz kopiert wird. Stattdessen werden die übertragenen Dateien und Ordner dem Benutzer und der Gruppe des Access Points zugewiesen. IDs In diesem Fall schlägt die

Aufgabenüberprüfung fehlt, da DataSync eine Diskrepanz zwischen den Metadaten im Quell- und Zielverzeichnis festgestellt wird.

Inhalt

- [Eine DataSync IAM-Rolle für den Dateisystemzugriff erstellen](#)
- [Beispiel für eine Dateisystemrichtlinie, die DataSync den Zugriff ermöglicht](#)

Eine DataSync IAM-Rolle für den Dateisystemzugriff erstellen

Wenn Sie über ein Amazon EFS-Dateisystem verfügen, das den Zugriff über eine IAM-Richtlinie einschränkt, können Sie eine IAM-Rolle erstellen, die das Lesen oder Schreiben von Daten aus dem Dateisystem ermöglicht DataSync . Möglicherweise müssen Sie diese Rolle dann in Ihrer [Dateisystemrichtlinie](#) angeben.

Um die DataSync IAM-Rolle zu erstellen

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen und dann Rolle erstellen aus.
3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus.
4. Fügen Sie den folgenden JSON-Code in den Richtlinien-Editor ein:

JSON

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

5. Wählen Sie Weiter aus. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
6. Geben Sie Ihrer Rolle einen Namen und wählen Sie Rolle erstellen aus.

Diese Rolle geben Sie bei der [Erstellung Ihres Standorts an](#).

Beispiel für eine Dateisystemrichtlinie, die DataSync den Zugriff ermöglicht

Die folgende Beispiel-Dateisystemrichtlinie zeigt, wie der Zugriff auf ein Amazon EFS-Dateisystem (in der Richtlinie als gekennzeichnet `fs-1234567890abcdef0`) eingeschränkt ist, aber dennoch den Zugriff DataSync über eine IAM-Rolle mit dem Namen `MyDataSyncRole` ermöglicht:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "ExampleEFSFileSystemPolicy",
  "Statement": [{
    "Sid": "AccessEFSFileSystem",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyDataSyncRole"
    },
    "Action": [
      "elasticfilesystem:ClientMount",
      "elasticfilesystem:ClientWrite",
      "elasticfilesystem:ClientRootAccess"
    ],
    "Resource": "arn:aws:elasticfilesystem:us-east-1:111122223333:file-system/fs-1234567890abcdef0",
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "true"
      },
      "StringEquals": {
        "elasticfilesystem:AccessPointArn":
          "arn:aws:elasticfilesystem:us-east-1:111122223333:access-point/fsap-abcdef01234567890"
      }
    }
  }]
}
```

```
}
```

- **Principal**— Gibt eine [IAM-Rolle](#) an, die die DataSync Erlaubnis zum Zugriff auf das Dateisystem erteilt.
- **Action**— Gewährt DataSync Root-Zugriff und ermöglicht das Lesen aus dem Dateisystem und das Schreiben in das Dateisystem.
- **aws:SecureTransport**— Erfordert, dass NFS-Clients TLS verwenden, wenn sie sich mit dem Dateisystem verbinden.
- **elasticfilesystem:AccessPointArn**— Erlaubt den Zugriff auf das Dateisystem nur über einen bestimmten Zugriffspunkt.

Überlegungen zum Netzwerk bei Amazon EFS-Übertragungen

VPCs die Sie mit verwenden, DataSync muss über eine Standardmandantenfähigkeit verfügen. VPCs mit Dedicated Tenancy werden nicht unterstützt.

Überlegungen zur Leistung bei Amazon EFS-Übertragungen

Der Durchsatzmodus Ihres Amazon EFS-Dateisystems kann die Übertragungsdauer und die Dateisystemleistung während der Übertragung beeinflussen. Berücksichtigen Sie dabei Folgendes:

- Für optimale Ergebnisse empfehlen wir die Verwendung des Elastic Throughput-Modus. Wenn Sie den Elastic Throughput-Modus nicht verwenden, kann Ihre Übertragung länger dauern.
- Wenn Sie den Bursting-Durchsatzmodus verwenden, kann die Leistung der Anwendungen Ihres Dateisystems beeinträchtigt werden, da Burst-Credits im Dateisystem DataSync verbraucht werden.
- Die Art und Weise, wie Sie [DataSync die Überprüfung Ihrer übertragenen Daten konfigurieren](#), kann sich auf die Leistung des Dateisystems und die Datenzugriffskosten auswirken.

Weitere Informationen finden Sie unter [Amazon EFS-Leistung](#) im Amazon Elastic File System-Benutzerhandbuch und auf der Seite mit den [Amazon EFS-Preisen](#).

Ihren Amazon EFS-Übertragungsort erstellen

Um den Übertragungsort zu erstellen, benötigen Sie ein vorhandenes Amazon EFS-Dateisystem. Falls Sie noch keinen haben, finden Sie weitere Informationen unter [Erste Schritte mit Amazon EFS](#) im Amazon Elastic File System-Benutzerhandbuch.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Speicherorttyp Amazon EFS-Dateisystem aus.

Sie konfigurieren diesen Speicherort später als Quelle oder Ziel.

4. Wählen Sie unter Dateisystem das Amazon EFS-Dateisystem aus, das Sie als Speicherort verwenden möchten.
5. Geben Sie unter Bereitstellungspfad einen Bereitstellungspfad für Ihr Amazon EFS-Dateisystem ein.

Dies gibt an, wo Daten in Ihrem Dateisystem DataSync gelesen oder geschrieben werden (je nachdem, ob es sich um einen Quell- oder Zielort handelt).

DataSync Verwendet standardmäßig das Stammverzeichnis (oder den [Access Point](#), falls Sie einen für die EFS-Zugriffspunkteinstellung angeben). Sie können Unterverzeichnisse auch mit Schrägstrichen angeben (z. B. /path/to/directory).

6. Wählen Sie unter Subnetz ein Subnetz aus, in dem Sie die [Netzwerkschnittstellen](#) für die Verwaltung Ihres Datenübertragungsverkehrs erstellen möchten DataSync .

Befinden muss sich das Subnetz:

- In derselben VPC wie Ihr Dateisystem.
- In derselben Availability Zone wie mindestens ein Dateisystem-Mount-Ziel.

Note

Sie müssen kein Subnetz angeben, das ein Bereitstellungsziel für das Dateisystem enthält.

- Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppe aus, die dem Mount-Ziel Ihres Amazon EFS-Dateisystems zugeordnet ist. Sie können mehr als eine Sicherheitsgruppe auswählen.

 Note

Die von Ihnen angegebenen Sicherheitsgruppen müssen eingehenden Datenverkehr auf dem NFS-Port 2049 zulassen. Weitere Informationen finden Sie unter [Ermitteln des Subnetzes und der Sicherheitsgruppen für Ihr Mount-Ziel](#).

- Wählen Sie für die Verschlüsselung während der Übertragung aus, ob Sie DataSync die Transport Layer Security (TLS) -Verschlüsselung für die Übertragung von Daten zu oder von Ihrem Dateisystem verwenden möchten.

 Note

Sie müssen diese Einstellung aktivieren, um einen Access Point, eine IAM-Rolle oder beides mit Ihrem Amazon EFS-Standort zu konfigurieren.

- (Optional) Wählen Sie für den EFS-Zugriffspunkt einen Zugriffspunkt aus, über den Sie Ihr Dateisystem mounten DataSync können.

Weitere Informationen finden Sie unter [Zugriff auf eingeschränkte Dateisysteme](#).

- (Optional) Geben Sie für die IAM-Rolle eine Rolle an, die DataSync den Zugriff auf Ihr Dateisystem ermöglicht.

Informationen zum Anlegen dieser Rolle finden Sie unter [Eine DataSync IAM-Rolle für den Dateisystemzugriff erstellen](#).

- (Optional) Wählen Sie Tag hinzufügen aus, um Ihr Dateisystem zu kennzeichnen.

Ein Tag ist ein Schlüssel/Wert-Paar, das Ihnen hilft, Ihre Speicherorte zu verwalten, zu filtern und zu suchen.

- Wählen Sie „Speicherort erstellen“.

Verwenden Sie den AWS CLI

- Kopieren Sie den folgenden `create-location-efs` Befehl:

```
aws datasync create-location-efs \
```



```
--efs-filesystem-arn 'arn:aws:elasticfilesystem:region:account-id:file-
system/file-system-id' \
--subdirectory /path/to/your/subdirectory \
--ec2-config SecurityGroupArns='arn:aws:ec2:region:account-id:security-
group/security-group-id',SubnetArn='arn:aws:ec2:region:account-id:subnet/subnet-id'
\
--in-transit-encryption TLS1_2 \
--access-point-arn 'arn:aws:elasticfilesystem:region:account-id:access-
point/access-point-id' \
--file-system-access-role-arn 'arn:aws:iam::account-id:role/datasync-efs-
access-role'
```

2. Geben Sie für `--efs-filesystem-arn` den Amazon-Ressourcennamen (ARN) des Amazon EFS-Dateisystems an, zu dem oder von dem Sie Daten übertragen.
3. Geben Sie für `--subdirectory` einen Bereitstellungspfad für Ihr Dateisystem an.

Hier werden Daten in Ihrem Dateisystem DataSync gelesen oder geschrieben (je nachdem, ob es sich um einen Quell- oder Zielort handelt).

DataSync verwendet standardmäßig das Stammverzeichnis (oder den [Access Point](#), falls Sie einen angeben `--access-point-arn`). Sie können Unterverzeichnisse auch mit Schrägstrichen angeben (z. B. `/path/to/directory`).

4. Als `--ec2-config` führen Sie Folgendes aus:
 - Geben Sie für den ARN der Sicherheitsgruppe an `SecurityGroupArns`, die dem Mount-Ziel Ihres Dateisystems zugeordnet ist. Sie können mehr als eine Sicherheitsgruppe angeben.

Note

Die von Ihnen angegebenen Sicherheitsgruppen müssen eingehenden Datenverkehr auf dem NFS-Port 2049 zulassen. Weitere Informationen finden Sie unter [Ermitteln des Subnetzes und der Sicherheitsgruppen für Ihr Mount-Ziel](#).

- Geben Sie für den ARN des Subnetzes an `SubnetArn`, in dem Sie die [Netzwerkschnittstellen](#) für die Verwaltung Ihres Datenübertragungsverkehrs erstellen möchten DataSync.

Befinden muss sich das Subnetz:

- In derselben VPC wie Ihr Dateisystem.
- In derselben Availability Zone wie mindestens ein Dateisystem-Mount-Ziel.

 Note

Sie müssen kein Subnetz angeben, das ein Bereitstellungsziel für das Dateisystem enthält.

5. Geben Sie für `--in-transit-encryption`, ob Sie DataSync die Transport Layer Security (TLS) -Verschlüsselung verwenden möchten, wenn Daten zu oder von Ihrem Dateisystem übertragen werden.

 Note

Sie müssen dies auf `tls1_2` um einen Access Point, eine IAM-Rolle oder beides mit Ihrem Amazon EFS-Standort zu konfigurieren.

6. (Optional) Geben Sie für `--access-point-arn` den ARN eines Access Points an, den Sie zum Mounten Ihres Dateisystems verwenden DataSync können.

Weitere Informationen finden Sie unter [Zugriff auf eingeschränkte Dateisysteme](#).

7. (Optional) Geben Sie für `--file-system-access-role-arn` den ARN einer IAM-Rolle an, die DataSync den Zugriff auf Ihr Dateisystem ermöglicht.

Informationen zum Anlegen dieser Rolle finden Sie unter [Eine DataSync IAM-Rolle für den Dateisystemzugriff erstellen](#).

8. Führen Sie den Befehl `create-location-efs` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN des Speicherorts anzeigt, den Sie erstellt haben. Beispiel:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Konfiguration von Übertragungen mit FSx für Windows File Server

Um Daten zu oder von Ihrem Amazon FSx for Windows File Server-Dateisystem zu übertragen, müssen Sie einen AWS DataSync Übertragungsort erstellen. DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bereitstellung des DataSync Zugriffs auf Dateisysteme FSx für Windows-Dateiserver

DataSync [stellt über das SMB-Protokoll \(Server Message Block\) eine Verbindung zu Ihrem Dateisystem FSx für Windows File Server her und mountet es mithilfe von Netzwerkschnittstellen von Ihrer Virtual Private Cloud \(VPC\) aus.](#)

Note

VPCs, die Sie mit verwenden, DataSync muss über eine Standardmandantenfähigkeit verfügen. VPCs mit Dedicated Tenancy werden nicht unterstützt.

Themen

- [Erforderliche Berechtigungen](#)
- [Erforderliche Authentifizierungsprotokolle](#)
- [DFS-Namespaces](#)

Erforderliche Berechtigungen

Sie müssen DataSync einem Benutzer die erforderlichen Rechte zum Mounten und Zugreifen auf Ihre Dateien, Ordner und Dateimetadaten FSx für Windows File Server gewähren.

Wir empfehlen, dass dieser Benutzer zu einer Microsoft Active Directory-Gruppe für die Verwaltung Ihres Dateisystems gehört. Die Besonderheiten dieser Gruppe hängen von Ihrem Active Directory-Setup ab:

- Wenn Sie AWS Directory Service for Microsoft Active Directory with FSx für Windows File Server verwenden, muss der Benutzer Mitglied der Gruppe AWS Delegierte FSx Administratoren sein.
- Wenn Sie selbstverwaltetes Active Directory mit FSx für Windows File Server verwenden, muss der Benutzer Mitglied einer von zwei Gruppen sein:
 - Die Gruppe Domänen-Admins, die Standardgruppe für delegierte Administratoren.

- Eine benutzerdefinierte Gruppe delegierter Administratoren mit Benutzerrechten, die das Kopieren von Objektbesitzberechtigungen und Windows-Zugriffskontrolllisten (ACLs) ermöglichen DataSync .

Important

Sie können die Gruppe der delegierten Administratoren nicht mehr ändern, nachdem das Dateisystem bereitgestellt wurde. Sie müssen das Dateisystem entweder erneut bereitstellen oder es aus einer Sicherung wiederherstellen, um die benutzerdefinierte delegierte Administratorgruppe mit den folgenden Benutzerrechten verwenden zu können, die Metadaten kopieren DataSync muss.

Benutzerrecht	Description
Dateien und Verzeichnisse wiederherstellen (SE_RESTORE_NAME)	Ermöglicht DataSync das Kopieren von Objekteigentümern, Berechtigungen, Dateimetadaten und beliebigen NTFS-Zugriffskontrolllisten (DACLs). Dieses Benutzerrecht wird normalerweise Mitgliedern der Gruppen Domänen-Admins und Backup-Operatoren gewährt (beide sind Active Directory-Standardgruppen).
Überwachungs- und Sicherheitsprotokoll verwalten (SE_SECURITY_NAME)	Ermöglicht DataSync das Kopieren von NTFS-Systemzugriffskontrolllisten (SACLs). Dieses Benutzerrecht wird normalerweise Mitgliedern der Gruppe Domänen-Admins gewährt.

- Wenn Sie Windows kopieren möchten ACLs und Daten zwischen einem SMB-Dateiserver und FSx dem Dateisystem Windows File Server oder zwischen Dateisystemen FSx für Windows File Server übertragen, DataSync müssen die von Ihnen angegebenen Benutzer derselben Active Directory-Domäne angehören oder über eine Active Directory-Vertrauensstellung zwischen ihren Domänen verfügen.

 Warning

Der SYSTEM-Benutzer Ihres Dateisystems FSx für Windows File Server muss über Vollzugriff auf alle Ordner in Ihrem Dateisystem verfügen. Ändern Sie nicht die NTFS-ACL-Berechtigungen für diesen Benutzer in Ihren Ordnern. Wenn Sie dies tun, DataSync können Sie die Berechtigungen Ihres Dateisystems so ändern, dass auf Ihre Dateifreigabe nicht mehr zugegriffen werden kann und Dateisystemsicherungen nicht verwendet werden können. Weitere Informationen zum Zugriff auf Datei- und Ordner Ebene finden Sie im [Amazon FSx for Windows File Server-Benutzerhandbuch](#).

Erforderliche Authentifizierungsprotokolle

Ihr Dateiserver FSx für Windows muss die NTLM-Authentifizierung verwenden, DataSync um darauf zugreifen zu können. DataSync kann nicht auf einen Dateiserver zugreifen, der die Kerberos-Authentifizierung verwendet.

DFS-Namespaces

DataSync unterstützt keine Microsoft Distributed File System (DFS) -Namespaces. Wir empfehlen, bei der Erstellung Ihres Standorts stattdessen einen zugrunde liegenden Dateiserver oder eine Dateifreigabe anzugeben. DataSync

Weitere Informationen finden Sie unter [Gruppierung mehrerer Dateisysteme mit DFS-Namespaces](#) im Amazon FSx for Windows File Server-Benutzerhandbuch.

Erstellen Sie Ihren Übertragungsort FSx für Windows File Server

Bevor Sie beginnen, stellen Sie sicher, dass Sie einen vorhandenen Dateiserver FSx für Windows in Ihrem AWS-Region haben. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon FSx](#) im Amazon FSx for Windows File Server-Benutzerhandbuch.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp Amazon aus FSx.

4. Wählen Sie als FSx Dateisystem das Dateisystem FSx für Windows File Server aus, das Sie als Speicherort verwenden möchten.
5. Geben Sie unter Freigabename einen Bereitstellungspfad FSx für Ihren Windows-Dateiserver mit Schrägstrichen ein.

Dies gibt den Pfad an, in den Daten DataSync gelesen oder geschrieben werden (je nachdem, ob es sich um einen Quell- oder Zielspeicherort handelt).

Sie können auch Unterverzeichnisse einbeziehen (z. B. /path/to/directory).

6. Wählen Sie für Sicherheitsgruppen bis zu fünf EC2 Amazon-Sicherheitsgruppen aus, die Zugriff auf das bevorzugte Subnetz Ihres Dateisystems ermöglichen.

Die von Ihnen ausgewählten Sicherheitsgruppen müssen in der Lage sein, mit den Sicherheitsgruppen Ihres Dateisystems zu kommunizieren. Informationen zur Konfiguration von Sicherheitsgruppen für den Dateisystemzugriff finden Sie im [Amazon FSx for Windows File Server-Benutzerhandbuch](#).

 Note

Wenn Sie eine Sicherheitsgruppe wählen, die keine internen Verbindungen zulässt, gehen Sie wie folgt vor:

- Konfigurieren Sie die Sicherheitsgruppe so, dass sie mit sich selbst kommunizieren kann.
- Wählen Sie eine andere Sicherheitsgruppe, die mit der Sicherheitsgruppe des Mount-Ziels kommunizieren kann.

7. Geben Sie unter Benutzer den Namen eines Benutzers ein, der auf Ihren FSx Windows-Dateiserver zugreifen kann.

Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

8. Geben Sie unter Passwort das Passwort des Benutzernamens ein.
9. (Optional) Geben Sie unter Domäne den Namen der Windows-Domäne ein, zu der Ihr Dateisystem FSx für Windows File Server gehört.

Wenn Sie mehrere Active Directory-Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieser Einstellung sichergestellt, dass die DataSync Verbindung zum richtigen Dateisystem hergestellt wird.

10. (Optional) Geben Sie Werte für die Felder Schlüssel und Wert ein, um sie FSx für den Windows-Dateiserver zu kennzeichnen.

Mithilfe von Tags können Sie Ihre AWS Ressourcen verwalten, filtern und nach ihnen suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

11. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

Um einen Speicherort FSx für Windows-Dateiserver zu erstellen, verwenden Sie AWS CLI

- Verwenden Sie den folgenden Befehl, um einen FSx Amazon-Standort zu erstellen.

```
aws datasync create-location-fsx-windows \
  --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system/filesystem-id \
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
  --user smb-user --password password
```

Gehen Sie im `create-location-fsx-windows` Befehl wie folgt vor:

- `fsx-filesystem-arn`— Geben Sie den Amazon-Ressourcennamen (ARN) des Dateisystems an, zu dem oder von dem Sie Daten übertragen möchten.
- `security-group-arns`— Geben Sie die ARNs von bis zu fünf EC2 Amazon-Sicherheitsgruppen an, die den Zugriff auf das bevorzugte Subnetz Ihres Dateisystems ermöglichen.

Die von Ihnen angegebenen Sicherheitsgruppen müssen in der Lage sein, mit den Sicherheitsgruppen Ihres Dateisystems zu kommunizieren. Informationen zur Konfiguration von Sicherheitsgruppen für den Dateisystemzugriff finden Sie im [Amazon FSx for Windows File Server-Benutzerhandbuch](#).

 Note

Wenn Sie eine Sicherheitsgruppe wählen, die keine internen Verbindungen zulässt, gehen Sie wie folgt vor:

- Konfigurieren Sie die Sicherheitsgruppe so, dass sie mit sich selbst kommunizieren kann.

- Wählen Sie eine andere Sicherheitsgruppe, die mit der Sicherheitsgruppe des Mount-Ziels kommunizieren kann.
- Die AWS-Region — Die Region, die Sie angeben, ist die, in der sich Ihr FSx Amazon-Zieldateisystem befindet.

Der Befehl gibt einen Speicherort-ARN ähnlich dem folgenden zurück.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07db7abfc326c50fb"
}
```

DataSync Transfers mit FSx for Lustre konfigurieren

Um Daten zu oder von Ihrem Amazon FSx for Lustre-Dateisystem zu übertragen, müssen Sie einen AWS DataSync Übertragungsort erstellen. DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bereitstellung des DataSync Zugriffs auf FSx Dateisysteme von For Lustre

DataSync greift mithilfe des Lustre-Clients auf Ihr FSx for Lustre-Dateisystem zu. DataSyncbenötigt Zugriff auf alle Daten auf Ihrem FSx for Lustre-Dateisystem. Um diese Zugriffsebene zu haben, hängen DataSync Sie Ihr Dateisystem als Root-Benutzer mit einer Benutzer-ID (UID) und einer Gruppen-ID (GID) von ein. 0

DataSync mountet Ihr Dateisystem mithilfe von [Netzwerkschnittstellen](#) aus Ihrer Virtual Private Cloud (VPC). DataSync verwaltet die Erstellung, Verwendung und Löschung dieser Netzwerkschnittstellen vollständig in Ihrem Namen.

Note

VPCs die Sie mit verwenden, DataSync muss über eine Standardmandantenfähigkeit verfügen. VPCs mit Dedicated Tenancy werden nicht unterstützt.

Erstellen Sie Ihren FSx Transferstandort für Lustre

Um den Übertragungsort zu erstellen, benötigen Sie ein FSx für Lustre vorhandenes Dateisystem. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon FSx for Lustre](#) im Amazon FSx for Lustre-Benutzerhandbuch.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter. <https://console.aws.amazon.com/datasync/>
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp Amazon aus FSx.

Sie konfigurieren diesen Speicherort später als Quelle oder Ziel.

4. Wählen Sie als FSx Dateisystem das FSx for Lustre-Dateisystem aus, das Sie als Speicherort verwenden möchten.
5. Geben Sie unter Mount-Pfad den Mount-Pfad für Ihr FSx for Lustre-Dateisystem ein.

Der Pfad kann ein Unterverzeichnis beinhalten. Wenn der Speicherort als Quelle verwendet wird, DataSync liest Daten aus dem Mount-Pfad. Wenn der Speicherort als Ziel verwendet wird, werden alle Daten in den Mount-Pfad DataSync geschrieben. Wenn kein Unterverzeichnis angegeben wird, wird das Stammverzeichnis (/) DataSync verwendet.

6. Wählen Sie für Sicherheitsgruppen bis zu fünf Sicherheitsgruppen aus, die den Zugriff auf Ihr FSx for Lustre-Dateisystem ermöglichen.

Die Sicherheitsgruppen müssen auf die Ports des Dateisystems zugreifen können. Das Dateisystem muss auch den Zugriff von den Sicherheitsgruppen aus ermöglichen.

Weitere Informationen zu Sicherheitsgruppen finden Sie unter [File System Access Control with Amazon VPC](#) im Amazon FSx for Lustre-Benutzerhandbuch.

7. (Optional) Geben Sie Werte für die Felder Schlüssel und Wert ein, um das FSx for Lustre-Dateisystem zu kennzeichnen.

Mithilfe von Tags können Sie Ihre AWS Ressourcen verwalten, filtern und nach ihnen suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

8. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

Um einen Standort FSx für Lustre zu erstellen, verwenden Sie AWS CLI

- Verwenden Sie den folgenden Befehl, um einen Standort FSx für Lustre zu erstellen.

```
aws datasync create-location-fsx-lustre \  
  --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system:filesystem-id \  
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id
```

Die folgenden Parameter sind für den `create-location-fsx-lustre` Befehl erforderlich.

- `fsx-filesystem-arn`— Der vollqualifizierte Amazon-Ressourcenname (ARN) des Dateisystems, aus dem Sie lesen oder in das Sie schreiben möchten.
- `security-group-arns`— Der ARN einer EC2 Amazon-Sicherheitsgruppe, der auf die [Netzwerkschnittstellen](#) des bevorzugten Subnetzes des Dateisystems angewendet werden soll.

Der vorherige Befehl gibt einen Standort-ARN zurück, der dem folgenden ähnelt.

```
{  
  "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/  
loc-07sb7abfc326c50fb"  
}
```

Konfiguration von DataSync Übertragungen mit Amazon FSx für OpenZFS

Um Daten zu oder von Ihrem Amazon FSx for OpenZFS-Dateisystem zu übertragen, müssen Sie einen AWS DataSync Übertragungsort erstellen. DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bereitstellung des DataSync Zugriffs auf FSx OpenZFS-Dateisysteme

DataSync [mountet Ihr FSx für OpenZFS-Dateisystem aus Ihrer Virtual Private Cloud \(VPC\) mithilfe von Netzwerkschnittstellen](#). DataSyncverwaltet die Erstellung, Verwendung und Löschung dieser Netzwerkschnittstellen vollständig in Ihrem Namen.

 Note

VPCs die Sie mit verwenden, DataSync muss über eine Standardmandantenfähigkeit verfügen. VPCs mit Dedicated Tenancy werden nicht unterstützt.

Konfiguration FSx für die OpenZFS-Dateisystemautorisierung

DataSync greift als NFS-Client auf Ihr Dateisystem FSx für OpenZFS zu und mountet das Dateisystem als Root-Benutzer mit einer Benutzer-ID (UID) und Gruppen-ID (GID) von. 0

DataSync Um all Ihre Datei-Metadaten zu kopieren, müssen Sie die NFS-Exporteinstellungen auf Ihren Dateisystem-Volumes mithilfe von konfigurieren. `no_root_squash` Sie können diese Zugriffsebene jedoch nur auf eine bestimmte DataSync Aufgabe beschränken.

Weitere Informationen finden Sie unter [Volume-Eigenschaften](#) im Amazon FSx for OpenZFS-Benutzerhandbuch.

Spezifische Konfiguration von NFS-Exporten für (empfohlen DataSync)

Sie können einen spezifischen NFS-Export für jedes Volume konfigurieren, auf das nur Ihre DataSync Task zugreift. Tun Sie dies für das neueste Vorgänger-Volume des Mount-Pfads, den Sie bei der Erstellung Ihres Standorts FSx für OpenZFS angeben.

Um einen NFS-Export zu konfigurieren, der spezifisch ist für DataSync

1. Erstellen Sie Ihre [DataSyncAufgabe](#).

Dadurch werden die Netzwerkschnittstellen der Aufgabe erstellt, die Sie in Ihren NFS-Exporteinstellungen angeben.

2. Suchen Sie die privaten IP-Adressen der Netzwerkschnittstellen der Aufgabe mithilfe der EC2 Amazon-Konsole oder AWS CLI.
3. Konfigurieren Sie FSx für Ihr OpenZFS-Dateisystem-Volume die folgenden NFS-Exporteinstellungen für jede Netzwerkschnittstelle der Aufgabe:
 - Client-Adresse: Geben Sie die private IP-Adresse der Netzwerkschnittstelle ein (z. B.).
10.24.34.0
 - NFS-Optionen: Geben Sie ein `rw,no_root_squash`.

Konfiguration von NFS-Exporten für alle Clients

Sie können einen NFS-Export angeben, der Root-Zugriff auf alle Clients ermöglicht.

Um einen NFS-Export für alle Clients zu konfigurieren

- Konfigurieren Sie FSx für Ihr OpenZFS-Dateisystemvolume die folgenden NFS-Exporteinstellungen:
 - Client-Adresse: Geben Sie ein. *
 - NFS-Optionen: Geben Sie ein `rw,no_root_squash`.

Erstellen Sie Ihren FSx Übertragungsort für OpenZFS

Um den Speicherort zu erstellen, benötigen Sie ein FSx für OpenZFS vorhandenes Dateisystem. Falls Sie noch keinen haben, finden Sie weitere Informationen unter [Erste Schritte mit Amazon FSx for OpenZFS](#) im Amazon FSx for OpenZFS-Benutzerhandbuch.

Verwenden der DataSync-Konsole

1. Öffnen Sie die Konsole unter AWS DataSync <https://console.aws.amazon.com/datasync/>
2. Wählen Sie im linken Navigationsbereich Standorte und dann Standort erstellen aus.
3. Wählen Sie als Standorttyp Amazon aus FSx.

Sie konfigurieren diesen Speicherort später als Quelle oder Ziel.

4. Wählen Sie als FSx Dateisystem das Dateisystem FSx für OpenZFS aus, das Sie als Speicherort verwenden möchten.
5. Geben Sie unter Mount-Pfad den Mount-Pfad FSx für Ihr OpenZFS-Dateisystem ein.

Der Pfad muss mit einem beliebigen Verzeichnispfad im Dateisystem beginnen `/fsx` und kann ein beliebiger vorhandener Verzeichnispfad sein. Wenn der Speicherort als Quelle verwendet wird, DataSync liest Daten aus dem Mount-Pfad. Wenn der Speicherort als Ziel verwendet wird, werden alle Daten in den Mount-Pfad DataSync geschrieben. Wenn kein Unterverzeichnis angegeben ist, wird das Stammverzeichnis des Volumes DataSync verwendet (z. B. `/fsx`).

6. Wählen Sie für Sicherheitsgruppen bis zu fünf Sicherheitsgruppen aus, die den Netzwerkzugriff auf Ihr FSx OpenZFS-Dateisystem ermöglichen.

Die Sicherheitsgruppen müssen Zugriff auf die Netzwerkports gewähren, die vom FSx for OpenZFS-Dateisystem verwendet werden. Das Dateisystem muss den Netzwerkzugriff von den Sicherheitsgruppen aus ermöglichen.

Weitere Informationen zu Sicherheitsgruppen finden Sie unter [Dateisystemzugriffskontrolle mit Amazon VPC](#) im Amazon FSx for OpenZFS-Benutzerhandbuch.

7. (Optional) Erweitern Sie Zusätzliche Einstellungen und wählen Sie für die NFS-Version die NFS-Version aus, die für den Zugriff auf Ihr Dateisystem DataSync verwendet wird.

DataSync Verwendet standardmäßig NFS-Version 4.1.

8. (Optional) Geben Sie Werte für die Felder Schlüssel und Wert ein, um das FSx OpenZFS-Dateisystem zu kennzeichnen.

Mithilfe von Stichwörtern können Sie Ihren Standort verwalten, filtern und danach suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

9. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

Um einen Speicherort FSx für OpenZFS zu erstellen, verwenden Sie AWS CLI

1. Kopieren Sie den folgenden Befehl: `create-location-fsx-open-zfs`

```
aws datasync create-location-fsx-open-zfs \
  --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system/filesystem-id \
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
  --protocol NFS={}
```

2. Geben Sie die folgenden erforderlichen Optionen im Befehl an:

- Geben Sie für `fsx-filesystem-arn` den vollqualifizierte Amazon-Ressourcennamen (ARN) des Standortdateisystems an. Dazu gehören der AWS-Region Speicherort Ihres Dateisystems AWS-Konto, Ihre und die Dateisystem-ID.
- Geben Sie für `security-group-arns` den ARN der EC2 Amazon-Sicherheitsgruppe an, die den Zugriff auf die [Netzwerkschnittstellen](#) des von Ihnen FSx für OpenZFS bevorzugten Subnetzes ermöglicht. Dazu gehören der AWS-Region Standort Ihrer EC2 Amazon-Instance AWS-Konto, Ihre und die Sicherheitsgruppen-ID.

Weitere Informationen zu Sicherheitsgruppen finden Sie unter [File System Access Control with Amazon VPC](#) im Amazon FSx for OpenZFS-Benutzerhandbuch.

- Geben Sie für das Protokoll `anprotocol`, das für den Zugriff auf Ihr Dateisystem DataSync verwendet wird. (unterstützt DataSync derzeit nur NFS.)
3. Führen Sie den Befehl aus. Sie erhalten eine Antwort mit dem Standort, den Sie gerade erstellt haben.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890"
}
```

Konfiguration von Übertragungen mit Amazon FSx für NetApp ONTAP

Um Daten zu oder von Ihrem Amazon FSx for NetApp ONTAP-Dateisystem zu übertragen, müssen Sie einen AWS DataSync Übertragungsort erstellen. DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bereitstellung des DataSync Zugriffs FSx auf ONTAP-Dateisysteme

Um auf ein FSx für ONTAP Dateisystem zuzugreifen, DataSync mounten Sie mithilfe von [Netzwerkschnittstellen](#) in Ihrer Virtual Private Cloud (VPC) eine virtuelle Speichermaschine (SVM) auf Ihrem Dateisystem. DataSync erstellt diese Netzwerkschnittstellen nur dann im bevorzugten Subnetz Ihres Dateisystems, wenn Sie eine Aufgabe erstellen, die Ihren Standort für ONTAP enthält. FSx

Note

VPCs die Sie mit verwenden, DataSync muss über eine Standardmandantenfähigkeit verfügen. VPCs mit Dedicated Tenancy werden nicht unterstützt.

DataSync kann mithilfe des Network File System (NFS) - oder Server Message Block (SMB) - Protokolls eine FSx Verbindung zur SVM eines ONTAP-Dateisystems herstellen und Daten kopieren.

Themen

- [Verwenden des NFS-Protokolls](#)
- [Verwenden des SMB-Protokolls](#)

- [Nicht unterstützte Protokolle](#)
- [Das richtige Protokoll wählen](#)
- [SnapLockZugreifen auf Volumes](#)

Verwenden des NFS-Protokolls

DataSync verwendet beim NFS-Protokoll den AUTH_SYS Sicherheitsmechanismus mit einer Benutzer-ID (UID) und einer Gruppen-ID (GID) von, um sich bei Ihrer SVM 0 zu authentifizieren.

Note

DataSync unterstützt derzeit nur NFS Version 3 mit vier ONTAP-Standorten. FSx

Verwenden des SMB-Protokolls

DataSync verwendet beim SMB-Protokoll die Anmeldeinformationen, die Sie zur Authentifizierung bei Ihrer SVM angeben.

Unterstützte SMB-Versionen

Wählt standardmäßig DataSync automatisch eine Version des SMB-Protokolls auf der Grundlage der Verhandlungen mit Ihrem SMB-Dateiserver aus. Sie können auch die Verwendung einer bestimmten Version konfigurieren, aber wir empfehlen, dies nur dann DataSync zu tun, wenn Sie Probleme haben, DataSync automatisch mit dem SMB-Dateiserver zu verhandeln. Aus Sicherheitsgründen empfehlen wir die Verwendung von SMB Version 3.0.2 oder höher.

In der folgenden Tabelle finden Sie eine Liste der Optionen in der DataSync Konsole und in der API für die Konfiguration einer SMB-Version mit Ihrem FSx ONTAP-Standort:

Konsolenoption	API-Option	Description
Automatisch	AUTOMATIC	DataSync und der SMB-Dateiserver handeln zwischen 2.1 und 3.1.1 die höchste Version von SMB aus, die sie gegenseitig unterstützen. Dies ist die Standardoption und die empfohlene Option. Wenn Sie stattdessen eine bestimmte Version auswählen, die Ihr Dateiserver nicht unterstützt,

Konsolenoption	API-Option	Description
		erhalten Sie möglicherweise eine Operation Not Supported -Fehlermeldung.
SMB 3.0.2	SMB3	Beschränkt die Protokollaushandlung nur auf SMB-Version 3.0.2.
SMB 2.1	SMB2	Beschränkt die Protokollaushandlung nur auf SMB-Version 2.1.
SMB 2.0	SMB2_0	Beschränkt die Protokollaushandlung nur auf SMB Version 2.0.

Erforderliche Berechtigungen

Sie müssen DataSync einem lokalen Benutzer in Ihrer SVM oder einem Domänenbenutzer in Ihrem Microsoft Active Directory die erforderlichen Rechte zum Mounten und Zugreifen auf Ihre Dateien, Ordner und Dateimetadaten gewähren.

Beachten Sie Folgendes, wenn Sie einen Benutzer in Ihrem Active Directory angeben:

- Wenn Sie verwenden AWS Directory Service for Microsoft Active Directory, muss der Benutzer Mitglied der Gruppe AWS Delegierte FSx Administratoren sein.
- Wenn Sie ein selbstverwaltetes Active Directory verwenden, muss der Benutzer Mitglied einer von zwei Gruppen sein:
 - Die Gruppe der Domänen-Admins, die Standardgruppe für delegierte Administratoren.
 - Eine benutzerdefinierte Gruppe delegierter Administratoren mit Benutzerrechten, die das Kopieren von Objektbesitzberechtigungen und Windows-Zugriffskontrolllisten () ermöglichen DataSync . ACLs

Important

Sie können die Gruppe der delegierten Administratoren nicht mehr ändern, nachdem das Dateisystem bereitgestellt wurde. Sie müssen das Dateisystem entweder erneut bereitstellen oder es aus einer Sicherung wiederherstellen, um die benutzerdefinierte delegierte Administratorgruppe mit den folgenden Benutzerrechten verwenden zu können, die Metadaten kopieren DataSync muss.

Benutzerrecht	Description
Als Teil des Betriebssystems agieren (SE_TCB_NAME)	Ermöglicht DataSync das Kopieren von Objekteigentümern, Berechtigungen, Dateimetadaten und beliebigen NTFS-Zugriffslisten (DACLs). Dieses Benutzerrecht wird normalerweise Mitgliedern der Gruppen Domänen-Admins und Backup-Operatoren gewährt (beide sind Active Directory-Standardgruppen).
Überwachungs- und Sicherheitsprotokoll verwalten () SE_SECURITY_NAME	Ermöglicht DataSync das Kopieren von NTFS-Systemzugriffskontrolllisten (SACLs). Dieses Benutzerrecht wird normalerweise Mitgliedern der Gruppe Domänen-Admins gewährt.

- Wenn Sie Windows kopieren möchten ACLs und zwischen FSx ONTAP-Dateisystemen mithilfe von SMB (oder anderen Arten von Dateisystemen, die SMB verwenden) wechseln möchten, DataSync müssen die von Ihnen angegebenen Benutzer derselben Active Directory-Domäne angehören oder über eine Active Directory-Vertrauensstellung zwischen ihren Domänen verfügen.

Erforderliche Authentifizierungsprotokolle

DataSync Um auf Ihren SMB-Share zugreifen zu können, muss Ihr FSx ONTAP-Dateisystem die NTLM-Authentifizierung verwenden. DataSync kann nicht auf ONTAP-Dateisysteme zugreifen, FSx die die Kerberos-Authentifizierung verwenden.

DFS-Namespaces

DataSync unterstützt keine Microsoft Distributed File System (DFS) -Namespaces. Wir empfehlen, bei der Erstellung Ihres Standorts stattdessen einen zugrunde liegenden Dateiserver oder eine Dateifreigabe anzugeben. DataSync

Nicht unterstützte Protokolle

DataSync kann nicht auf ONTAP-Dateisysteme zugreifen FSx , die das iSCSI-Protokoll (Internet Small Computer Systems Interface) verwenden.

Das richtige Protokoll wählen

Um Dateimetadaten FSx für ONTAP-Migrationen beizubehalten, konfigurieren Sie Ihre DataSync Quell- und Zielspeicherorte so, dass sie dasselbe Protokoll verwenden. Unter den unterstützten Protokollen bewahrt SMB Metadaten mit der höchsten Genauigkeit (weitere Informationen finden Sie unter). [Verstehen, wie DataSync mit Datei- und Objektmetadaten umgegangen wird](#)

Gehen Sie bei der Migration von einem Unix-Server (Linux) oder einer NAS-Freigabe (Network Attached Storage), die Benutzern über NFS zur Verfügung steht, wie folgt vor:

1. [Erstellen Sie einen NFS-Speicherort](#) für den Unix (Linux) -Server oder die NAS-Freigabe. (Dies wird Ihr Quellspeicherort sein.)
2. Konfigurieren Sie das FSx ONTAP-Volume, auf das Sie Daten übertragen, mit dem [Unix-Sicherheitsstil](#).
3. Erstellen Sie einen Speicherort FSx für Ihr ONTAP-Dateisystem, das für NFS konfiguriert ist. (Dies wird Ihr Zielort sein.)

Gehen Sie bei der Migration von einem Windows-Server oder einer NAS-Freigabe, die Benutzer über SMB bedient, wie folgt vor:

1. [Erstellen Sie einen SMB-Standort](#) für den Windows-Server oder die NAS-Freigabe. (Dies wird Ihr Quellstandort sein.)
2. Konfigurieren Sie das FSx ONTAP-Volume, auf das Sie Daten übertragen, mit dem [NTFS-Sicherheitsstil](#).
3. Erstellen Sie einen Speicherort FSx für Ihr ONTAP-Dateisystem, das für SMB konfiguriert ist. (Dies wird Ihr Zielort sein.)

Wenn Ihre FSx für ONTAP Umgebung mehrere Protokolle verwendet, empfehlen wir die Zusammenarbeit mit einem AWS Speicherspezialisten. Weitere Informationen zu bewährten Methoden für den Multiprotokollzugriff finden Sie unter [Aktivieren von Multiprotokoll-Workloads mit Amazon FSx](#) für ONTAP. NetApp

SnapLockZugreifen auf Volumes

Wenn Sie Daten auf ein [SnapLock Volume](#) auf einem FSx für ONTAP Dateisystem übertragen, stellen Sie sicher, dass die SnapLock Einstellungen Autocommit und Volume Append Mode auf dem Volume während der Übertragung deaktiviert sind. Sie können diese Einstellungen wieder aktivieren, wenn Sie mit der Datenübertragung fertig sind.

Erstellen Sie Ihren FSx Übertragungsort für ONTAP

Um den Speicherort zu erstellen, benötigen Sie ein FSx für ONTAP vorhandenes Dateisystem. Falls Sie noch keinen haben, finden Sie weitere Informationen unter [Erste Schritte mit Amazon FSx for NetApp ONTAP](#) im Amazon FSx for NetApp ONTAP-Benutzerhandbuch.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter. <https://console.aws.amazon.com/datasync/>
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp Amazon aus FSx.

Sie konfigurieren diesen Speicherort später als Quelle oder Ziel.

4. Wählen Sie als FSx Dateisystem das FSx für ONTAP geeignete Dateisystem aus, das Sie als Speicherort verwenden möchten.
5. Wählen Sie für virtuelle Speichermaschine eine virtuelle Speichermaschine (SVM) in Ihrem Dateisystem aus, in die Sie Daten kopieren möchten oder von der Sie Daten kopieren möchten.
6. Geben Sie unter Bereitstellungspfad einen Pfad zur Dateifreigabe auf der SVM an, in die Sie Ihre Daten kopieren werden.

Sie können einen Knotenpfad (auch als Mount-Punkt bezeichnet), einen Qtree-Pfad (für NFS-Dateifreigaben) oder einen Share-Namen (für SMB-Dateifreigaben) angeben. Ihr Mount-Pfad könnte zum Beispiel /vol1, /vol1/tree1 oder /share1 sein.

Tip

Geben Sie keinen Pfad im Root-Volume der SVM an. Weitere Informationen finden Sie unter [Verwaltung FSx virtueller ONTAP-Speichermaschinen](#) im Amazon FSx for NetApp ONTAP-Benutzerhandbuch.

7. Wählen Sie für Sicherheitsgruppen bis zu fünf EC2 Amazon-Sicherheitsgruppen aus, die Zugriff auf das bevorzugte Subnetz Ihres Dateisystems ermöglichen.

Die Sicherheitsgruppen müssen ausgehenden Datenverkehr an den folgenden Ports zulassen (abhängig vom verwendeten Protokoll):

- NFS — TCP-Ports 111, 635 und 2049
- SMB — TCP-Anschluss 445

Die Sicherheitsgruppen Ihres Dateisystems müssen auch eingehenden Datenverkehr über dieselben Ports zulassen.

8. Wählen Sie unter Protokoll das Datenübertragungsprotokoll aus, das für den Zugriff auf die SVM Ihres Dateisystems DataSync verwendet wird.

Weitere Informationen finden Sie unter [Das richtige Protokoll wählen](#).

NFS

DataSync verwendet NFS Version 3.

SMB

Konfigurieren Sie eine SMB-Version, einen Benutzer, ein Passwort und einen Active Directory-Domänennamen (falls erforderlich) für den Zugriff auf die SVM.

- (Optional) Erweitern Sie Zusätzliche Einstellungen und wählen Sie eine SMB-Version für den DataSync Zugriff auf Ihre SVM aus.

Wählt standardmäßig DataSync automatisch eine Version aus, die auf den Verhandlungen mit dem SMB-Dateiserver basiert. Weitere Informationen finden Sie unter [Verwenden des SMB-Protokolls](#).

- Geben Sie im Feld Benutzer einen Benutzernamen ein, der die Dateien, Ordner und Metadaten, die Sie auf die SVM übertragen möchten, bereitstellen und darauf zugreifen kann.

Weitere Informationen finden Sie unter [Verwenden des SMB-Protokolls](#).

- Geben Sie im Feld Passwort das Passwort des angegebenen Benutzers ein, der auf die SVM zugreifen kann.

- (Optional) Geben Sie für den Active Directory-Domänennamen den vollqualifizierten Domänennamen (FQDN) des Active Directory-Verzeichnisses ein, zu dem Ihre SVM gehört.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, stellen Sie durch die Konfiguration dieser Einstellung sicher, dass die DataSync Verbindung zur richtigen SVM hergestellt wird.

9. (Optional) Geben Sie Werte für die Felder Schlüssel und Wert ein, um das FSx ONTAP-Dateisystem zu kennzeichnen.

Mithilfe von Tags können Sie Ihre AWS Ressourcen verwalten, filtern und nach ihnen suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

10. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

Um einen Standort FSx für ONTAP zu erstellen, verwenden Sie AWS CLI

1. Kopieren Sie den folgenden `create-location-fsx-ontap` Befehl:

```
aws datasync create-location-fsx-ontap \
  --storage-virtual-machine-arn arn:aws:fsx:region:account-id:storage-virtual-
machine/fs-file-system-id \
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
  --protocol data-transfer-protocol={}
```

2. Geben Sie die folgenden erforderlichen Optionen im Befehl an:

- Geben Sie für `storage-virtual-machine-arn` den vollqualifizierten Amazon-Ressourcennamen (ARN) einer virtuellen Speichermaschine (SVM) in Ihrem Dateisystem an, in die Sie Daten kopieren möchten oder von der Sie Daten kopieren möchten.

Dieser ARN beinhaltet den AWS-Region Speicherort Ihres Dateisystems, Ihr AWS-Konto Dateisystem, das Dateisystem und die IDs SVM.

- Geben Sie für `security-group-arns` die ARNs EC2 Amazon-Sicherheitsgruppen an, die den Zugriff auf die [Netzwerkschnittstellen](#) des bevorzugten Subnetzes Ihres Dateisystems ermöglichen.

Dazu gehören der AWS-Region Standort Ihrer EC2 Amazon-Instance AWS-Konto, Ihre und Ihre Sicherheitsgruppe IDs. Sie können bis zu fünf Sicherheitsgruppen ARNs angeben.

Weitere Informationen zu Sicherheitsgruppen finden Sie unter [File System Access Control with Amazon VPC](#) im Amazon FSx for NetApp ONTAP User Guide.

- Konfigurieren Sie zum `protocol` Beispiel das Protokoll, das für den Zugriff auf die SVM Ihres Dateisystems DataSync verwendet wird.
- Für NFS können Sie die Standardkonfiguration verwenden:

```
--protocol NFS={}
```

- Für SMB müssen Sie einen Benutzernamen und ein Passwort für den Zugriff auf die SVM angeben:

```
--protocol SMB={User=smb-user, Password=smb-password}
```

3. Führen Sie den Befehl aus.

Sie erhalten eine Antwort, in der der Standort angezeigt wird, den Sie gerade erstellt haben.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890"
}
```

Übertragung zu oder von einem anderen Cloud-Speicher mit AWS DataSync

Mit AWS DataSync können Sie Daten zwischen einigen anderen Cloud-Anbietern und AWS Speicherdiensten übertragen. Weitere Informationen finden Sie unter [Wohin kann ich meine Daten übertragen DataSync?](#)

Themen

- [Planung von Übertragungen zu oder von Cloud-Speichersystemen von Drittanbietern](#)
- [AWS DataSync Übertragungen mit Google Cloud Storage konfigurieren](#)
- [Transfers konfigurieren mit Microsoft Azure Blob Storage](#)
- [AWS DataSync Transfers konfigurieren mit Microsoft Azure Files SMB-Aktien](#)

- [Konfiguration von Übertragungen mit anderem Cloud-Objektspeicher](#)

Planung von Übertragungen zu oder von Cloud-Speichersystemen von Drittanbietern

Beachten Sie bei der Planung cloudübergreifender Datenübertragungen Folgendes:

- Verwendung eines Agenten: Ein Agent muss nur dann auf Speicher in anderen Clouds zugreifen, wenn Aufgaben im Basismodus verwendet werden. Für [Aufgaben im erweiterten Modus](#) ist kein Agent erforderlich. Wenn Sie sich für die Verwendung eines Agenten entscheiden, können Sie ihn bei der Übertragung aus dem S3-kompatiblen Objektspeicher eines Cloud-Anbieters als [EC2Amazon-Instance](#) oder als Google Compute Engine bzw. Azure Virtual Machine für Übertragungen von diesen spezifischen Speicherdiensten bereitstellen. Bei der Übertragung von Dateisystemen in Google und Azure empfehlen wir, den Agenten als Google- oder Azure-VM bereitzustellen, sodass sich der Agent so nah wie möglich am Dateisystem befindet. Darüber hinaus werden die Daten vom Agenten auf DataSync komprimiert AWS, wodurch die Kosten für ausgehenden Datenverkehr gesenkt werden können. DataSync bietet eine Liste [validierter Cloud-Standorte](#), die die erforderliche [Amazon S3 S3-API-Kompatibilität](#) bieten.
- Der Objektspeicher-Endpunkt der anderen Cloud: Der Speicherendpunkt für einen Cloud-Drittanbieter ist in der Regel region- oder kontospezifisch. Der regionale Endpunkt wird zusammen mit einem angegebenen Bucket-Namen als Server am DataSync Objektspeicherort verwendet.
- Speicherklassen der Quellobjekte: Wie Amazon S3 unterstützen einige Cloud-Anbieter eine Archivschicht, die eine Wiederherstellung erfordert, bevor auf die archivierten Objekte zugegriffen werden kann. Beispielsweise müssen Objekte in der Azure BLOB-Archivschicht vor einer Datenübertragung für den Standardzugriff abgerufen werden. Auf Objekte in der Google Cloud Storage-Archivschicht kann sofort zugegriffen werden und sie müssen nicht wiederhergestellt werden. Allerdings fallen im Zusammenhang mit dem direkten Zugriff auf die Archivebene Abrufkosten an. Bevor Sie mit der Datenübertragung beginnen, lesen Sie in der Dokumentation zu Ihrer Cloud-übergreifenden Speicherklasse die Zugriffsanforderungen und Abrufgebühren. Weitere Informationen zum Wiederherstellen archivierter Objekte in Amazon S3 finden Sie unter [Wiederherstellen eines archivierten Objekts](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- Zugriff auf Objektspeicher: Für die Übertragung von Daten zwischen Cloud-Drittanbietern ist der Zugriff auf den Objektspeicher der anderen Cloud in Form von Authentifizierungsschlüsseln erforderlich. Um beispielsweise Zugriff auf Google Cloud Storage zu gewähren, konfigurieren Sie einen DataSync Objektspeicherort, der eine Verbindung zur [Google Cloud Storage-XML-API](#)

herstellt und sich mithilfe eines [Hash-basierten HMAC-Schlüssels \(Message Authentication Code\)](#) für Ihr Dienstkonto authentifiziert. [Für Azure Blob Storage konfigurieren Sie einen dedizierten Azure DataSync Blob-Speicherort, der mithilfe von SAS-Token authentifiziert wird.](#) DataSync verwendet AWS Secrets Manager, um Ihre Objektspeicher-Anmeldeinformationen sicher zu speichern. Weitere Informationen finden Sie unter [Sichern der Anmeldeinformationen für den Speicherort](#).

- Unterstützung für Objekt-Tags:
 - Im Gegensatz zu Amazon S3 unterstützen nicht alle Cloud-Anbieter [Objekt-Tags](#). DataSync Aufgaben können beim Versuch, Tags vom Quellspeicherort zu lesen, fehlschlagen, wenn der Cloud-Anbieter keine Objekt-Tags über die Amazon S3 S3-API unterstützt oder wenn die von Ihnen angegebenen Anmeldeinformationen nicht ausreichen, um die Tags abzurufen. DataSync bietet eine Aufgabenoption zum Deaktivieren des [Lesens und Kopierens von Objekt-Tags](#) während einer Übertragung, wenn Objekt-Tags nicht unterstützt werden oder Sie die Tags nicht behalten möchten. Lesen Sie in der Dokumentation Ihres Cloud-Anbieters nach, ob Objekt-Tags unterstützt werden, und überprüfen Sie die Objekt-Tag-Einstellungen Ihrer Übertragungsaufgabe, bevor Sie die Übertragung starten.
 - Sie können die Amazon S3 S3-API verwenden, um zu überprüfen, ob ein Cloud-Anbieter eine `get-object-tagging` Anfrage zurückgibt. Weitere Informationen finden Sie unter [get-object-tagging](#) in der Referenz zum AWS CLI -Befehl.

Ein Cloud-Anbieter, der Objekt-Tags unterstützt, gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint-url=https://
BUCKET_ENDPOINT --key prefix/file1

{
    "TagSet": []
}
```

Ein Cloud-Anbieter, der dies nicht unterstützt `get-object-tagging`, gibt die folgende Meldung zurück:

```
aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint-url=https://
BUCKET_ENDPOINT --key prefix/file1
```


An error occurred (OperationNotSupported) when calling the GetObjectTagging operation: The operation is not supported for this resource

- Damit verbundene Kosten für Anfragen und ausgehende Daten: Beim Übertragen von Daten aus dem Cloud-Objektspeicher [fallen Kosten für Anfragen](#) und ausgehende Daten an. Die Gebühren für Anfragen variieren je nach Cloud-Anbieter und gegebenenfalls zwischen Speicherklassen. Informationen zu den spezifischen Kosten für Anfragen im Verhältnis zur Speicherklasse, aus der Sie lesen möchten, finden Sie in der Dokumentation Ihres Cloud-Anbieters. Eine Übersicht über die Gebühren, die DataSync für Datenübertragungen anfallen, finden Sie unter [Bewertung der Kosten für S3-Anfragen bei der Nutzung DataSync](#) und [AWS DataSync Preisgestaltung](#). Bei der Übertragung von Daten von bestimmten Cloud-Anbietern fallen Gebühren für ausgehenden Datenverkehr an. Die Kosten für die Datenübertragung variieren zwischen den Cloud-Anbietern und hängen auch von der Region ab, in der die Daten gespeichert sind.
- Anforderungsraten für Objektspeicher: Cloud-Anbieter weisen für ihre Objektspeicherplattformen unterschiedliche Leistungs- und Anforderungsratenmerkmale auf. Prüfen Sie die Anforderungsraten Ihres anderen Cloud-Anbieters und ermitteln Sie, wo die Anforderungslimits gelten. Planen Sie im Voraus für stark parallelisierte Übertragungen, die aus mehreren Agenten bestehen und bei denen möglicherweise spezifische Partitionierungen oder Leistungssteigerungen erforderlich sind.

Amazon S3 verfügt über dokumentierte Anforderungsraten, auf die Sie Ihre Lösung aufbauen können. Die Amazon S3 S3-Anforderungsraten gelten pro partitioniertem Präfix und sind auf mehrere Präfixe skalierbar. Weitere Informationen finden Sie unter [Bewährte Entwurfsmuster: Optimierung der Amazon S3 S3-Leistung](#) im Amazon Simple Storage Service-Benutzerhandbuch.

AWS DataSync Übertragungen mit Google Cloud Storage konfigurieren

Mit AWS DataSync können Sie Daten zwischen Google Cloud Storage und den folgenden AWS Speicherdiensten übertragen:

- Amazon S3
- Amazon EFS
- Amazon FSx für Windows-Dateiserver
- Amazon FSx für Lustre
- Amazon FSx für OpenZFS
- Amazon FSx für NetApp ONTAP

Um mit der Einrichtung der Übertragung zu beginnen, erstellen Sie einen Speicherort für Ihren Google Cloud Storage. Dieser Standort kann entweder als Übertragungsquelle oder als Ziel für die Übertragung dienen. Ein DataSync Agent ist nur erforderlich, wenn Sie Daten zwischen Google Cloud Storage und Amazon EFS oder Amazon FSx übertragen oder wenn Sie Aufgaben im Basismodus verwenden. Für Datenübertragungen im erweiterten Modus zwischen Google Cloud Storage und Amazon S3 ist kein Agent erforderlich.

 Note

Verwenden Sie für private Cloud-Konnektivität zwischen Google Cloud Storage und AWS den Basismodus mit Agenten.

Übersicht

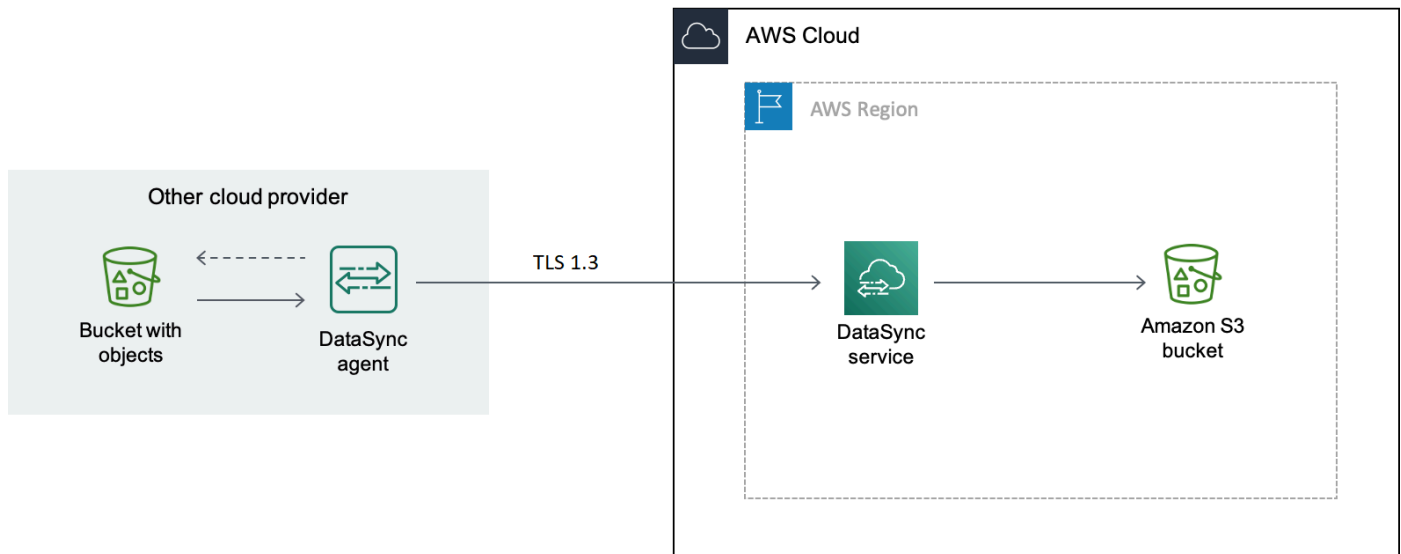
DataSync verwendet die [Google Cloud Storage-XML-API](#) für Datenübertragungen. Diese API bietet eine Amazon S3 S3-kompatible Schnittstelle zum Lesen und Schreiben von Daten mit Google Cloud Storage-Buckets.

Wenn Sie den Basismodus für Übertragungen verwenden, können Sie den Agenten in Google Cloud Storage oder Ihrer Amazon VPC bereitstellen.

Agent in Google Cloud

1. Sie stellen einen DataSync Agenten in Ihrer Google Cloud-Umgebung bereit.
2. Der Agent liest Ihren Google Cloud Storage-Bucket mithilfe eines Hash-basierten HMAC-Schlüssels (Message Authentication Code).
3. Die Objekte aus Ihrem Google Cloud Storage-Bucket werden mithilfe eines öffentlichen Endpunkts sicher über TLS 1.3 in den AWS Cloud übertragen.
4. Der DataSync Dienst schreibt die Daten in Ihren S3-Bucket.

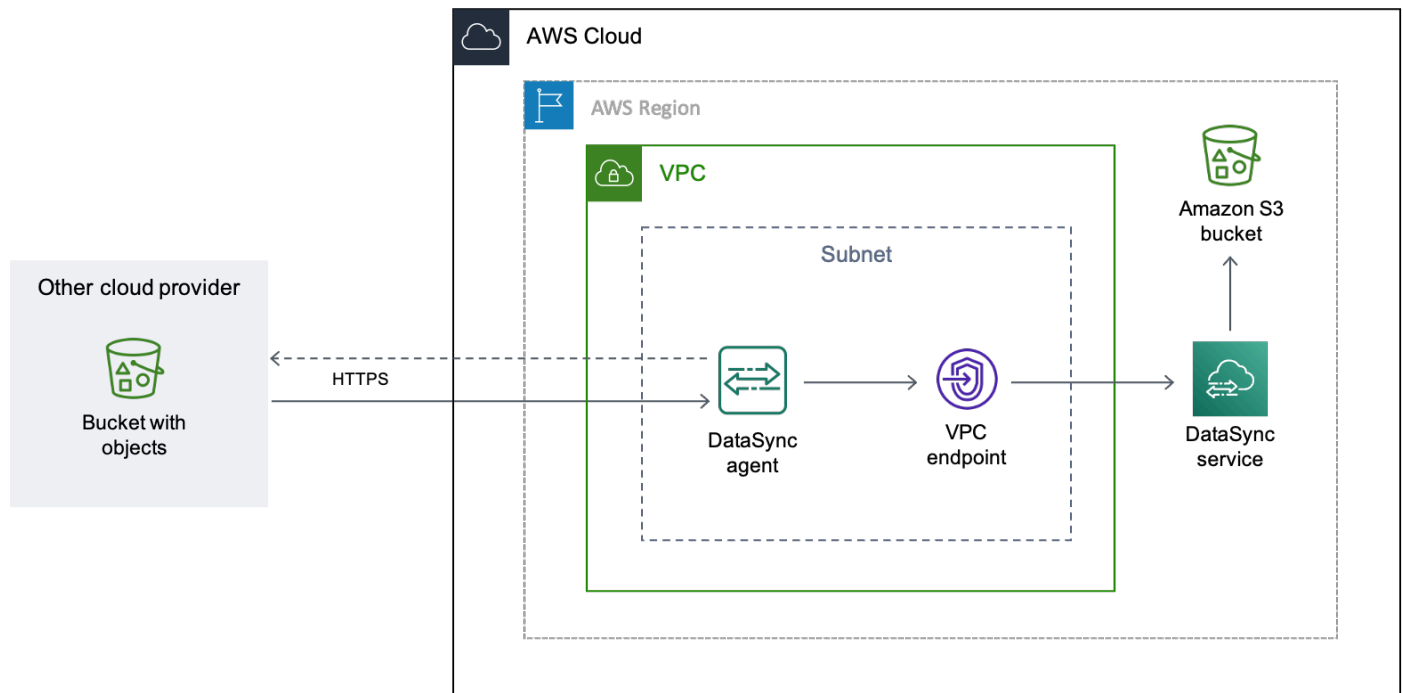
Das folgende Diagramm veranschaulicht die Übertragung.



Agent in your VPC

1. Sie stellen einen DataSync Agenten in einer Virtual Private Cloud (VPC) in Ihrer AWS Umgebung bereit.
2. Der Agent liest Ihren Google Cloud Storage-Bucket mithilfe eines Hash-basierten HMAC-Schlüssels (Message Authentication Code).
3. Die Objekte aus Ihrem Google Cloud Storage-Bucket werden AWS Cloud mithilfe eines privaten VPC-Endpunkts sicher über TLS 1.3 in den übertragen.
4. Der DataSync Dienst schreibt die Daten in Ihren S3-Bucket.

Das folgende Diagramm veranschaulicht die Übertragung.



Kosten

Die mit dieser Migration verbundenen Gebühren können Folgendes beinhalten:

- Ausführen einer Google [Compute Engine-Instanz](#) für virtuelle Maschinen (VM) (wenn Sie Ihren DataSync Agenten in Google Cloud bereitstellen)
- Ausführen einer [EC2Amazon-Instance](#) (wenn Sie Ihren DataSync Agenten in einer VPC innerhalb AWS bereitstellen)
- Übertragung der Daten über [DataSync](#), einschließlich der Gebühren für Anfragen im Zusammenhang mit [Google Cloud Storage](#) und [Amazon S3](#) (falls S3 einer Ihrer Übertragungsorte ist)
- Übertragung von Daten aus [Google Cloud Storage](#)
- Speichern von Daten in [Amazon S3](#)

Voraussetzungen

Bevor Sie beginnen, gehen Sie wie folgt vor, falls Sie dies noch nicht getan haben:

- [Erstellen Sie einen Google Cloud Storage-Bucket](#) mit den Objekten, in die Sie Daten übertragen möchten AWS.

- [Melde dich für eine an AWS-Konto.](#)
- [Erstellen Sie einen Amazon S3 S3-Bucket](#), in dem Sie Ihre Objekte speichern können, nachdem sie eingetroffen sind AWS.

Einen HMAC-Schlüssel für Ihren Google Cloud Storage-Bucket erstellen

DataSync verwendet einen HMAC-Schlüssel, der mit Ihrem Google-Dienstkonto verknüpft ist, um sich bei dem Bucket zu authentifizieren und den Bucket zu lesen, aus dem Sie Daten übertragen. (Eine ausführliche Anleitung zum Erstellen von HMAC-Schlüsseln finden Sie in der [Google Cloud Storage-Dokumentation](#).)

Um einen HMAC-Schlüssel zu erstellen

1. Erstellen Sie einen HMAC-Schlüssel für Ihr Google-Dienstkonto.
2. Stellen Sie sicher, dass Ihr Google-Dienstkonto mindestens über `Storage Object Viewer` Berechtigungen verfügt.
3. Speichern Sie die Zugriffs-ID und das Geheimnis Ihres HMAC-Schlüssels an einem sicheren Ort.

Sie benötigen diese Elemente später, um Ihren DataSync Quellstandort zu konfigurieren.

Schritt 2: Konfigurieren Sie Ihr Netzwerk

Die Netzwerkkonfiguration ist nur erforderlich, wenn Sie bei Ihrer Übertragung einen DataSync Agenten verwenden. Die Netzwerkanforderungen für diese Migration hängen davon ab, wo Sie Ihren Agenten einsetzen möchten.

Für einen DataSync Agenten in Google Cloud

Wenn Sie Ihren DataSync Agenten in Google Cloud hosten möchten, konfigurieren Sie Ihr Netzwerk so, [dass DataSync Übertragungen über einen öffentlichen Endpunkt](#) möglich sind.

Für einen DataSync Agenten in Ihrer VPC

Wenn Sie Ihren Agenten hosten möchten AWS, benötigen Sie eine VPC mit einem Schnittstellenendpunkt. DataSync verwendet den VPC-Endpunkt, um die Übertragung zu erleichtern.

So konfigurieren Sie Ihr Netzwerk für einen VPC-Endpunkt

1. Wenn Sie noch keine haben, [erstellen Sie eine VPC](#) in derselben Umgebung AWS-Region wie in Ihrem S3-Bucket.
2. [Erstellen Sie ein privates Subnetz für Ihre VPC](#).
3. [Erstellen Sie einen VPC-Serviceendpunkt](#) für DataSync.
4. Konfigurieren Sie Ihr Netzwerk so, [dass DataSync Übertragungen über einen VPC-Serviceendpunkt](#) möglich sind.

Ändern Sie dazu die [Sicherheitsgruppe](#), die Ihrem VPC-Dienstendpunkt zugeordnet ist.

Schritt 3: Erstellen Sie einen DataSync Agenten (optional)

Ein DataSync Agent ist nur erforderlich, wenn Sie Aufgaben im Basismodus verwenden. Wenn Sie den erweiterten Modus für die Übertragung zwischen Google Cloud Storage (GCS) und Amazon S3 verwenden, ist kein Agent erforderlich. Wenn Sie den Basismodus verwenden möchten, benötigen Sie einen DataSync Agenten, der auf Ihren GCS-Bucket zugreifen kann.

Für Google Cloud

In diesem Szenario wird der DataSync Agent in Ihrer Google Cloud-Umgebung ausgeführt.

Bevor Sie beginnen: [Installieren Sie die Google Cloud CLI](#).

Um den Agenten für Google Cloud zu erstellen

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich Agents und anschließend Create Agent aus.
3. Wählen Sie für Hypervisor die Option Image herunterladen aus VMware ESXi, um eine .zip Datei herunterzuladen, die den Agenten enthält.
4. Öffnen Sie ein -Terminalfenster. Entpacken Sie das Image, indem Sie den folgenden Befehl ausführen:

```
unzip AWS-DataSync-Agent-VMWare.zip
```

5. Extrahieren Sie den Inhalt der .ova Agentendatei, aws-datasync indem Sie zunächst den folgenden Befehl ausführen:

```
tar -xvf aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt.ova
```

6. Importieren Sie die .vmdk Agentendatei in Google Cloud, indem Sie den folgenden Google Cloud CLI-Befehl ausführen:

```
gcloud compute images import aws-datasync-2-test \  
  --source-file INCOMPLETE-aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt-disk1.vmdk \  
  --os centos-7
```

 Note

Das Importieren der .vmdk Datei kann bis zu zwei Stunden dauern.

7. Erstellen und starten Sie eine VM-Instanz für das Agenten-Image, das Sie gerade importiert haben.

Die Instanz benötigt die folgenden Konfigurationen für Ihren Agenten. (Eine ausführliche Anleitung zum Erstellen einer Instanz finden Sie in der [Google Cloud Compute Engine-Dokumentation](#).)

- Wählen Sie für den Maschinentyp eine der folgenden Optionen aus:
 - e2-standard-8 — Für DataSync Aufgabenausführungen, die mit bis zu 20 Millionen Objekten arbeiten.
 - e2-standard-16 — Für DataSync Aufgabenausführungen, die mit mehr als 20 Millionen Objekten arbeiten.
- Die Einstellungen für die Startdiskette finden Sie im Abschnitt Benutzerdefinierte Images. Wählen Sie dann das DataSync Agent-Image aus, das Sie gerade importiert haben.
- Wählen Sie für die Einstellungen für das Dienstkonto Ihr Google-Dienstkonto aus (dasselbe Konto, das Sie in [Schritt 1](#) verwendet haben).
- Wählen Sie für die Firewall-Einstellung die Option, um HTTP-Verkehr (Port 80) zuzulassen.

Um Ihren DataSync Agenten zu aktivieren, muss Port 80 auf dem Agenten geöffnet sein. Der Port muss nicht öffentlich zugänglich sein. Nach der Aktivierung wird der Port DataSync geschlossen.

8. Notieren Sie sich nach dem Ausführen der VM-Instanz ihre öffentliche IP-Adresse.

Sie benötigen diese IP-Adresse, um den Agenten zu aktivieren.

9. Gehen Sie zurück zur DataSync Konsole. Gehen Sie auf dem Bildschirm Create Agent (Agent erstellen), in den Sie das Agenten-Image heruntergeladen haben, wie folgt vor, um Ihren Agenten zu aktivieren:
 - Wählen Sie als Endpunkttyp die Option Public Service Endpoints aus (z. B. Public Service Endpoints in US East Ohio).
 - Wählen Sie unter Aktivierungsschlüssel die Option Automatisch den Aktivierungsschlüssel von Ihrem Agenten abrufen aus.
 - Geben Sie als Agentenadresse die öffentliche IP-Adresse der Agent-VM-Instanz ein, die Sie gerade erstellt haben.
 - Wählen Sie Schlüssel abrufen aus.
10. Geben Sie Ihrem Agenten einen Namen und wählen Sie dann Create Agent aus.

Ihr Agent ist online und bereit, Daten zu übertragen.

Für Ihre VPC

In diesem Szenario wird der Agent als EC2 Amazon-Instance in einer VPC ausgeführt, die mit Ihrer AWS-Konto verknüpft ist.

Bevor Sie beginnen: [Richten Sie die AWS Command Line Interface \(AWS CLI\) ein](#).

Um den Agenten für Ihre VPC zu erstellen

1. Öffnen Sie ein -Terminalfenster. Stellen Sie sicher, dass Sie Ihr AWS CLI Profil so konfigurieren, dass es das Konto verwendet, das Ihrem S3-Bucket zugeordnet ist.
2. Kopieren Sie den folgenden Befehl. *vpc-region* Ersetzen Sie durch den AWS-Region Ort, an dem sich Ihre VPC befindet (z. B. *us-east-1*).

```
aws ssm get-parameter --name /aws/service/datasync/ami --region vpc-region
```

3. Führen Sie den Befehl aus. Notieren Sie sich in der Ausgabe die "Value" Eigenschaft.

Dieser Wert ist die DataSync Amazon Machine Image (AMI) -ID der Region, die Sie angegeben haben. Eine AMI-ID könnte beispielsweise so aussehen `ami-1234567890abcdef0`.

4. Kopieren Sie die folgende URL. Ersetzen Sie erneut *vpc-region* durch den Ort, AWS-Region an dem sich Ihre VPC befindet. Ersetzen Sie es dann *ami-id* durch die AMI-ID, die Sie im vorherigen Schritt notiert haben.

```
https://console.aws.amazon.com/ec2/v2/home?region=vpc-region#LaunchInstanceWizard:ami=ami-id
```

5. Fügen Sie die URL in einen Browser ein.

Die Startseite der EC2 Amazon-Instance AWS-Managementkonsole wird angezeigt.

6. Wählen Sie unter Instance-Typ eine der [empfohlenen EC2 Amazon-Instances für DataSync Agenten](#) aus.
7. Wählen Sie für key pair ein vorhandenes Schlüsselpaar aus, oder erstellen Sie ein neues.
8. Wählen Sie unter Netzwerkeinstellungen die VPC und das Subnetz aus, in denen Sie den Agenten bereitstellen möchten.
9. Wählen Sie Launch Instance (Instance starten) aus.
10. Sobald die EC2 Amazon-Instance läuft, [wählen Sie Ihren VPC-Endpunkt](#) aus.
11. [Aktivieren Sie Ihren Agenten](#).

Schritt 4: Erstellen Sie einen DataSync Quellspeicherort für Ihren Google Cloud Storage-Bucket

Um einen DataSync Speicherort für Ihren Google Cloud Storage-Bucket einzurichten, benötigen Sie die Zugriffs-ID und das Geheimnis für den HMAC-Schlüssel, den Sie in [Schritt 1](#) erstellt haben.

Um den DataSync Quellspeicherort zu erstellen

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp die Option Objektspeicher aus.
4. Geben Sie für Server den Wert ein **storage.googleapis.com**.
5. Geben Sie als Bucket-Namen den Namen Ihres Google Cloud Storage-Buckets ein.
6. Geben Sie für Ordner ein Objektpräfix ein.

DataSync kopiert nur Objekte mit diesem Präfix.

7. Wenn für Ihre Übertragung ein Agent erforderlich ist, wählen Sie Agenten verwenden und dann den Agenten aus, den Sie in [Schritt 3](#) erstellt haben.
8. Erweitern Sie Additional settings (Zusätzliche Einstellungen). Wählen Sie für Serverprotokoll die Option HTTPS aus. Wählen Sie 443 für Serverport aus.
9. Scrollen Sie nach unten zum Abschnitt Authentifizierung. Vergewissern Sie sich, dass das Kontrollkästchen Anmeldeinformationen erforderlich aktiviert ist, und gehen Sie dann wie folgt vor:
 - Geben Sie unter Zugriffsschlüssel die Zugriffs-ID Ihres HMAC-Schlüssels ein.
 - Geben Sie unter Geheimer Schlüssel entweder den geheimen Schlüssel Ihres HMAC-Schlüssels direkt ein, oder geben Sie ein AWS Secrets Manager Geheimnis an, das den Schlüssel enthält. Weitere Informationen finden Sie unter [Bereitstellen von Anmeldeinformationen für Speicherorte](#).
10. Wählen Sie Standort erstellen aus.

Schritt 5: Erstellen Sie einen DataSync Zielort für Ihren S3-Bucket

Sie benötigen einen DataSync Ort, an dem Ihre Daten landen sollen.

Um den DataSync Zielort zu erstellen

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. [Erstellen Sie einen DataSync Standort für den S3-Bucket](#).

Wenn Sie den DataSync Agenten in Ihrer VPC bereitgestellt haben, wird in diesem Tutorial davon ausgegangen, dass sich der S3-Bucket in derselben AWS-Region VPC und DataSync Ihrem Agenten befindet.

Schritt 6: Erstellen und starten Sie eine Aufgabe DataSync

Wenn Ihre Quell- und Zielorte konfiguriert sind, können Sie damit beginnen, Ihre Daten dorthin zu verschieben AWS.

Um die DataSync Aufgabe zu erstellen und zu starten

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
 2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
 3. Gehen Sie auf der Seite Quellspeicherort konfigurieren wie folgt vor:
 - a. Wählen Sie „Bestehenden Standort auswählen“.
 - b. Wählen Sie den Quellspeicherort aus, den Sie in [Schritt 4](#) erstellt haben, und klicken Sie dann auf Weiter.
 4. Gehen Sie auf der Seite Zielort konfigurieren wie folgt vor:
 - a. Wählen Sie „Bestehenden Standort auswählen“.
 - b. Wählen Sie den Zielort aus, den Sie in [Schritt 5](#) erstellt haben, und klicken Sie dann auf Weiter.
 5. Gehen Sie auf der Seite „Einstellungen konfigurieren“ wie folgt vor:
 - a. Erweitern Sie unter Konfiguration der Datenübertragung den Eintrag Zusätzliche Einstellungen und deaktivieren Sie das Kontrollkästchen Objekt-Tags kopieren.
-
- Important**
- Da die Google Cloud Storage XML API das Lesen oder Schreiben von Objekt-Tags nicht unterstützt, schlägt Ihre DataSync Aufgabe möglicherweise fehl, wenn Sie versuchen, Objekt-Tags zu kopieren.
- b. Konfigurieren Sie alle anderen gewünschten Aufgabeneinstellungen und wählen Sie dann Weiter.
 6. Überprüfen Sie auf der Seite Überprüfen Ihre Einstellungen und wählen Sie dann Aufgabe erstellen aus.
 7. Wählen Sie auf der Detailseite der Aufgabe die Option Start und dann eine der folgenden Optionen aus:
 - Um die Aufgabe ohne Änderungen auszuführen, wählen Sie Mit Standardeinstellungen beginnen.
 - Um die Aufgabe vor der Ausführung zu ändern, wählen Sie Mit überschreibenden Optionen beginnen.

Wenn Ihre Aufgabe abgeschlossen ist, sehen Sie die Objekte aus Ihrem Google Cloud Storage-Bucket in Ihrem S3-Bucket.

Transfers konfigurieren mit Microsoft Azure Blob Storage

Mit AWS DataSync können Sie Daten zwischen Microsoft Azure Blob Storage (einschließlich Azure Data Lake Storage Gen2 Blob-Speicher) und den folgenden AWS Speicherdiensten übertragen:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Amazon FSx für Windows-Dateiserver](#)
- [Amazon FSx für Lustre](#)
- [Amazon FSx für OpenZFS](#)
- [Amazon FSx für NetApp ONTAP](#)

Um diese Art der Übertragung einzurichten, erstellen Sie einen [Standort](#) für Ihren Azure Blob Storage. Sie können diesen Standort als Übertragungsquelle oder Ziel verwenden. Ein DataSync Agent ist nur erforderlich, wenn Daten zwischen Azure Blob und Amazon EFS oder Amazon FSx übertragen werden oder wenn Aufgaben im Basismodus verwendet werden. Sie benötigen keinen Agenten, um Daten zwischen Azure Blob und Amazon S3 im erweiterten Modus zu übertragen.

Bereitstellung des DataSync Zugriffs auf Ihr Azure Blob Storage

Wie auf Sie DataSync zugegriffen wird, Azure Blob Storage hängt von mehreren Faktoren ab, z. B. davon, ob Sie Daten zu oder von einem Blob-Speicher übertragen und welche Art von [Shared Access Signature \(SAS\) -Token](#) Sie verwenden. Ihre Objekte müssen sich außerdem in einer [Zugriffsebene](#) befinden, mit der gearbeitet werden DataSync kann.

Themen

- [SAS-Token](#)
- [Zugriffsebenen](#)

SAS-Token

Ein SAS-Token gibt die Zugriffsberechtigungen für Ihren Blob-Speicher an. (Weitere Informationen zu SAS finden Sie in der [Azure Blob StorageDokumentation](#).)

Sie können SAS-Token generieren, um verschiedene Zugriffsebenen bereitzustellen. DataSync unterstützt Token mit den folgenden Zugriffsebenen:

- Account
- Container

Die benötigten Zugriffsberechtigungen hängen vom Umfang Ihres Tokens ab. DataSync Wenn Sie nicht über die richtigen Berechtigungen verfügen, kann Ihre Übertragung fehlschlagen. Ihre Übertragung ist beispielsweise nicht erfolgreich, wenn Sie Objekte mit Tags verschieben, Ihr SAS-Token Azure Blob Storage jedoch nicht über Tag-Berechtigungen verfügt.

Themen

- [SAS-Token-Berechtigungen für den Zugriff auf Kontoebene](#)
- [SAS-Token-Berechtigungen für den Zugriff auf Containerebene](#)
- [SAS-Ablaufrichtlinien](#)

SAS-Token-Berechtigungen für den Zugriff auf Kontoebene

DataSync benötigt ein Zugriffstoken auf Kontoebene mit den folgenden Berechtigungen (je nachdem, ob Sie zu oder von dort übertragen). Azure Blob Storage

Transfers from blob storage

- Zulässige Dienste — Blob
- Zulässige Ressourcentypen — Container, Objekt

Wenn Sie diese Berechtigungen nicht angeben, DataSync können Sie Ihre Objektmetadaten, einschließlich [Objekt-Tags](#), nicht übertragen.

- Zulässige Berechtigungen — Lesen, Auflisten
- Zulässige Blob-Index-Berechtigungen — [Lesen/Schreiben \(wenn Sie Objekt-Tags kopieren DataSync möchten\)](#)

Transfers to blob storage

- Zulässige Dienste — Blob
- Zulässige Ressourcentypen — Container, Objekt

Wenn Sie diese Berechtigungen nicht angeben, DataSync können Sie Ihre Objektmetadaten, einschließlich [Objekt-Tags](#), nicht übertragen.

- Zulässige Berechtigungen — Lesen, Schreiben, Auflisten, Löschen (wenn Sie Dateien entfernen DataSync möchten, die sich nicht in Ihrer Übertragungsquelle befinden)
- Zulässige Blob-Indexberechtigungen — [Lesen/Schreiben \(wenn Sie Objekt-Tags kopieren DataSync möchten\)](#)

SAS-Token-Berechtigungen für den Zugriff auf Containerebene

DataSync benötigt ein Zugriffstoken auf Containerebene mit den folgenden Berechtigungen (je nachdem, ob Sie zu oder von dort übertragen). Azure Blob Storage

Transfers from blob storage

- Lesen
- Auflisten
- Tag (wenn Sie [Objekt-Tags](#) kopieren DataSync möchten)

Note

Sie können die Tag-Berechtigung nicht hinzufügen, wenn Sie ein SAS-Token im Azure Portal generieren. Um die Tag-Berechtigung hinzuzufügen, generieren Sie stattdessen das Token mithilfe der [Azure Storage Explorer](#) App oder generieren Sie ein [SAS-Token, das Zugriff auf Kontoebene ermöglicht](#).

Transfers to blob storage

- Lesen
- Write (Schreiben)
- Auflisten
- Löschen (wenn Sie Dateien entfernen DataSync möchten, die sich nicht in Ihrer Übertragungsquelle befinden)
- Tag (wenn Sie [Objekt-Tags](#) kopieren DataSync möchten)

 Note

Sie können die Tag-Berechtigung nicht hinzufügen, wenn Sie ein SAS-Token im Azure Portal generieren. Um die Tag-Berechtigung hinzuzufügen, generieren Sie stattdessen das Token mithilfe der [Azure Storage Explorer](#) App oder generieren Sie ein [SAS-Token, das Zugriff auf Kontoebene ermöglicht](#).

SAS-Ablaufrichtlinien

Stellen Sie sicher, dass Ihr SAS nicht abläuft, bevor Sie damit rechnen, Ihre Übertragung abzuschließen. Informationen zur Konfiguration einer SAS-Ablaufrichtlinie finden Sie in der [Azure Blob StorageDokumentation](#).

Wenn das SAS während der Übertragung abläuft, DataSync kann nicht mehr auf Ihren Azure Blob Storage Standort zugegriffen werden. (Möglicherweise wird die Fehlermeldung „Verzeichnis konnte nicht geöffnet werden“ angezeigt.) In diesem Fall [aktualisieren Sie Ihren Standort](#) mit einem neuen SAS-Token und starten Sie Ihre DataSync Aufgabe neu.

Zugriffsebenen

Bei der Übertragung von Azure Blob Storage DataSync können Objekte der Stufen „Heiß“ und „Kalt“ kopiert werden. Bei Objekten in der Archivzugriffsebene müssen Sie diese Objekte in die Warm- oder Kaltstufe rehydrieren, bevor Sie sie kopieren können.

Bei der Übertragung auf Azure Blob Storage DataSync können Objekte in die Zugriffsebenen „Heiß“, „Kühl“ und „Archiv“ kopiert werden. Wenn Sie Objekte in die Archivzugriffsebene kopieren, DataSync kann die Übertragung nicht verifiziert werden, wenn Sie versuchen, [alle Daten im Ziel zu überprüfen](#).

DataSync unterstützt die Stufe für den kalten Zugriff nicht. Weitere Informationen zu den Zugriffsebenen finden Sie in der [Azure Blob StorageDokumentation](#).

Überlegungen zu Azure Blob Storage Übertragungen

Wenn Sie planen, Daten zu oder von Azure Blob Storage mit zu übertragen DataSync, sollten Sie einige Dinge beachten.

Themen

- [Kosten](#)

- [Blob-Typen](#)
- [AWS-Region -Verfügbarkeit](#)
- [Objekt-Tags werden kopiert](#)
- [Übertragung auf Amazon S3](#)
- [Löschen von Verzeichnissen in einem Übertragungsziel](#)
- [Einschränkungen](#)

Kosten

Die Gebühren, die mit der Übertragung von Daten in oder aus der Quelle verbunden sind, Azure Blob Storage können Folgendes beinhalten:

- Ausführen einer [Azurevirtuellen Maschine \(VM\)](#) (wenn Sie einen DataSync Agenten einsetzen Azure)
- Ausführen einer [EC2Amazon-Instance](#) (wenn Sie einen DataSync Agenten in einer VPC innerhalb AWS bereitstellen)
- Übertragung der Daten über Amazon S3 [DataSync](#), einschließlich der Anforderungsgebühren für [Amazon S3](#) (falls S3 einer Ihrer Übertragungsorte ist) [Azure Blob Storage](#)
- Übertragung von Daten in oder aus [Azure Blob Storage](#)
- Speichern von Daten in einem [AWS Speicherdienst](#), der unterstützt wird von DataSync

Blob-Typen

Wie mit Blob-Typen DataSync funktioniert, hängt davon ab, ob Sie zu oder von dort übertragen. Azure Blob Storage Wenn Sie Daten in den Blob-Speicher verschieben, können die Objekte oder Dateien, die DataSync übertragen werden, nur Block-Blobs sein. Wenn Sie Daten aus dem Blob-Speicher verschieben, DataSync können Blobs übertragen, blockiert, verschoben und angehängt werden.

[Weitere Informationen zu Blob-Typen finden Sie in der Dokumentation. Azure Blob Storage](#)

AWS-Region -Verfügbarkeit

Sie können einen Azure Blob Storage Übertragungsort an einem beliebigen Ort erstellen [AWS-Region](#) , [der von DataSync unterstützt wird](#).

Objekt-Tags werden kopiert

Die Fähigkeit DataSync, Objekt-Tags bei der Übertragung zu oder von dort beizubehalten, Azure Blob Storage hängt von den folgenden Faktoren ab:

- Die Größe der Tags eines Objekts — Objekte mit Tags, die 2 KB überschreiten, DataSync können nicht übertragen werden.
- Ob für DataSync das Kopieren von Objekt-Tags konfiguriert ist — DataSync [kopiert standardmäßig Objekt-Tags](#).
- Der Namespace, den Ihr Azure Speicherkonto verwendet — DataSync kann Objekttags kopieren, wenn Ihr Azure Speicherkonto einen flachen Namespace verwendet, aber nicht, wenn Ihr Konto einen hierarchischen Namespace verwendet (eine Funktion von). Azure Data Lake Storage Gen2 Ihre DataSync Aufgabe schlägt fehl, wenn Sie versuchen, Objekttags zu kopieren und Ihr Speicherkonto einen hierarchischen Namespace verwendet.
- Ob Ihr SAS-Token das Tagging autorisiert — Die Berechtigungen, die Sie zum Kopieren von Objekt-Tags benötigen, hängen von der Zugriffsebene ab, die Ihr Token bietet. Ihre Aufgabe schlägt fehl, wenn Sie versuchen, Objekt-Tags zu kopieren, und Ihr Token nicht über die richtigen Berechtigungen zum Taggen verfügt. Weitere Informationen finden Sie in den Berechtigungsanforderungen für Zugriffstoken auf [Kontoebene oder Zugriffstoken auf Containerebene](#).

Übertragung auf Amazon S3

Bei der Übertragung zu Amazon S3 DataSync werden keine Azure Blob Storage Objekte übertragen, die größer als 5 TB sind, oder Objekte mit Metadaten, die größer als 2 KB sind.

Löschen von Verzeichnissen in einem Übertragungsziel

Bei der Übertragung an Azure Blob Storage DataSync können [Objekte in Ihrem Blob-Speicher entfernt werden, die in Ihrer Übertragungsquelle nicht vorhanden](#) sind. (Sie können diese Option konfigurieren, indem Sie die Einstellung Gelöschte Dateien behalten in der DataSync Konsole löschen. Ihr [SAS-Token](#) muss außerdem über Löschberechtigungen verfügen.)

Wenn Sie Ihre Übertragung auf diese Weise konfigurieren, DataSync werden keine Verzeichnisse in Ihrem Blob-Speicher gelöscht, wenn Ihr Azure Speicherkonto einen hierarchischen Namespace verwendet. In diesem Fall müssen Sie die Verzeichnisse manuell löschen (z. B. mithilfe von). [Azure Storage Explorer](#)

Einschränkungen

Beachten Sie bei der Übertragung von oder nach Daten die folgenden Einschränkungen Azure Blob Storage:

- DataSync [erstellt einige Verzeichnisse](#) an einem Speicherort, um Ihnen die Übertragung zu erleichtern. Wenn Azure Blob Storage es sich um einen Zielort handelt und Ihr Speicherkonto einen hierarchischen Namespace verwendet, fallen Ihnen möglicherweise aufgabenspezifische Unterverzeichnisse (z. B. `task-000011112222abcde`) in dem Ordner auf. `/.aws-datasync` DataSync löscht diese Unterverzeichnisse in der Regel nach einer Übertragung. Geschieht das nicht, können Sie diese aufgabenspezifischen Verzeichnisse selbst löschen, solange eine Aufgabe nicht ausgeführt wird.
- DataSync unterstützt nicht die Verwendung eines SAS-Tokens, um nur auf einen bestimmten Ordner in Ihrem Azure Blob Storage Container zuzugreifen.
- Sie können kein SAS-Token für die Benutzerdelegierung für den Zugriff auf Ihren Blob-Speicher bereitstellen DataSync .

Erstellen Sie Ihren DataSync Agenten (optional)

Ein DataSync Agent ist nur erforderlich, wenn Daten zwischen Azure Blob und Amazon EFS oder Amazon FSx übertragen werden oder wenn Aufgaben im Basismodus verwendet werden. Sie benötigen keinen Agenten, um Daten zwischen Azure Blob und Amazon S3 im erweiterten Modus zu übertragen. In diesem Abschnitt wird beschrieben, wie Sie einen Agenten bereitstellen und aktivieren.

Tip

Sie können Ihren Agenten zwar auf einer EC2 Amazon-Instance einsetzen, die Verwendung eines Microsoft Hyper-V Agenten kann jedoch zu einer geringeren Netzwerklatenz und mehr Datenkomprimierung führen.

Microsoft Hyper-V-Agenten

Sie können Ihren DataSync Agenten direkt Azure mit einem Microsoft Hyper-V Image einsetzen.

 Tip

Bevor Sie fortfahren, sollten Sie in Erwägung ziehen, ein Shell-Skript zu verwenden, mit dem Sie Ihren Hyper-V-Agenten möglicherweise schneller bereitstellen können. Azure Weitere Informationen und das Herunterladen des Codes finden Sie unter [GitHub](#). Wenn Sie das Skript verwenden, können Sie mit dem Abschnitt über fortfahren [Den Aktivierungsschlüssel Ihres Agenten abrufen](#).

Themen

- [Voraussetzungen](#)
- [Ihren Agenten herunterladen und vorbereiten](#)
- [Bereitstellen Sie Ihren Agenten in Azure](#)
- [Den Aktivierungsschlüssel Ihres Agenten abrufen](#)
- [Ihren Agenten aktivieren](#)

Voraussetzungen

Um Ihren DataSync Agenten vorzubereiten und zu implementieren Azure, müssen Sie wie folgt vorgehen:

- Aktivieren Sie es Hyper-V auf Ihrem lokalen Computer.
- Installieren Sie [PowerShell](#) (einschließlich der Hyper-V Module).
- Installieren Sie die [Azure CLI](#).
- Installieren [AzCopy](#).

Ihren Agenten herunterladen und vorbereiten

Laden Sie einen Agenten von der DataSync Konsole herunter. Bevor Sie den Agenten bereitstellen können Azure, müssen Sie ihn in eine virtuelle Festplatte (VHD) mit fester Größe konvertieren. Weitere Informationen finden Sie in der [Azure-Dokumentation](#).

So laden Sie Ihren Agenten herunter und bereiten ihn vor

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.

2. Wählen Sie im linken Navigationsbereich Agents und anschließend Create Agent aus.
3. Wählen Sie für Hypervisor Microsoft Hyper-V die Option Image herunterladen aus.

Der Agent lädt eine .zip Datei herunter, die eine .vhdx Datei enthält.

4. Extrahieren Sie die .vhdx Datei auf Ihrem lokalen Computer.
5. Öffnen Sie PowerShell und führen Sie die folgenden Schritte aus:
 - a. Kopieren Sie das folgende Convert-VHD Cmdlet:

```
Convert-VHD -Path .\local-path-to-vhdx-file\aws-datasync-2.0.1686143940.1-  
x86_64.xfs.gpt.vhdx -  
-DestinationPath .\local-path-to-vhdx-file\aws-datasync-2016861439401-  
x86_64.vhd -VHDType Fixed
```

- b. Ersetzen Sie jede Instanz von *local-path-to-vhdx-file* durch den Speicherort der .vhdx Datei auf Ihrem lokalen Computer.
- c. Führen Sie den Befehl aus.

Ihr Agent ist jetzt eine virtuelle Festplatte mit fester Größe (mit einem .vhd Dateiformat) und kann dort bereitgestellt werden. Azure

Bereitstellen Sie Ihren Agenten in Azure

Der Einsatz Ihres DataSync Agenten in Azure umfasst:

- Erstellen einer verwalteten Festplatte in Azure
- Laden Sie Ihren Agenten auf diese verwaltete Festplatte hoch
- Die verwaltete Festplatte an eine Linux virtuelle Maschine anhängen

Um Ihren Agenten bereitzustellen in Azure

1. Gehen Sie in PowerShell das Verzeichnis, das die .vhd Datei Ihres Agenten enthält.
2. Führen Sie den ls Befehl aus und speichern Sie den Length Wert (z. B.85899346432).

Dies ist die Größe Ihres Agenten-Images in Byte, die Sie benötigen, wenn Sie eine verwaltete Festplatte erstellen, auf der das Image gespeichert werden kann.

3. Gehen Sie wie folgt vor, um eine verwaltete Festplatte zu erstellen:

- a. Kopieren Sie den folgenden Azure CLI-Befehl:

```
az disk create -n your-managed-disk `
-g your-resource-group `
-l your-azure-region `
--upload-type Upload `
--upload-size-bytes agent-size-bytes `
--sku standard_lrs
```

- b. *your-managed-disk* Ersetzen Sie ihn durch einen Namen für Ihre verwaltete Festplatte.
- c. *your-resource-group* Ersetzen Sie ihn durch den Namen der Azure Ressourcengruppe, zu der Ihr Speicherkonto gehört.
- d. *your-azure-region* Ersetzen Sie es durch die Azure Region, in der sich Ihre Ressourcengruppe befindet.
- e. *agent-size-bytes* Ersetzen Sie es durch die Größe Ihres Agentenbilds.
- f. Führen Sie den Befehl aus.

Dieser Befehl erstellt eine leere verwaltete Festplatte mit einer [Standard-SKU](#), auf die Sie Ihren DataSync Agenten hochladen können.

4. Gehen Sie wie folgt vor, um eine Shared Access Signature (SAS) zu generieren, die Schreibzugriff auf die verwaltete Festplatte ermöglicht:

- a. Kopieren Sie den folgenden Azure CLI-Befehl:

```
az disk grant-access -n your-managed-disk `
-g your-resource-group `
--access-level Write `
--duration-in-seconds 86400
```

- b. *your-managed-disk* Ersetzen Sie ihn durch den Namen der verwalteten Festplatte, die Sie erstellt haben.
- c. *your-resource-group* Ersetzen Sie es durch den Namen der Azure Ressourcengruppe, zu der Ihr Speicherkonto gehört.
- d. Führen Sie den Befehl aus.

Notieren Sie sich in der Ausgabe den SAS-URI. Sie benötigen diese URI, wenn Sie den Agenten auf Azure hochladen.

Mit dem SAS können Sie bis zu einer Stunde auf die Festplatte schreiben. Das bedeutet, dass Sie eine Stunde Zeit haben, um Ihren Agenten auf die verwaltete Festplatte hochzuladen.

5. Gehen Sie wie folgt vor, um Ihren Agenten auf Azure Ihre verwaltete Festplatte hochzuladen:

a. Kopieren Sie den folgenden AzCopy Befehl:

```
.\azcopy copy local-path-to-vhd-file sas-uri --blob-type PageBlob
```

b. *local-path-to-vhd-file* Ersetzen Sie ihn durch den Speicherort der .vhd Agentendatei auf Ihrem lokalen Computer.

c. *sas-uri* Ersetzen Sie durch den SAS-URI, den Sie bei der Ausführung des `az disk grant-access` Befehls erhalten haben.

d. Führen Sie den Befehl aus.

6. Wenn der Upload des Agenten abgeschlossen ist, widerrufen Sie den Zugriff auf Ihre verwaltete Festplatte. Kopieren Sie dazu den folgenden Azure CLI-Befehl:

```
az disk revoke-access -n your-managed-disk -g your-resource-group
```

a. *your-resource-group* Ersetzen Sie es durch den Namen der Azure Ressourcengruppe, zu der Ihr Speicherkonto gehört.

b. *your-managed-disk* Ersetzen Sie durch den Namen der verwalteten Festplatte, die Sie erstellt haben.

c. Führen Sie den Befehl aus.

7. Gehen Sie wie folgt vor, um Ihre verwaltete Festplatte an eine neue Linux VM anzuhängen:

a. Kopieren Sie den folgenden Azure CLI-Befehl:

```
az vm create --resource-group your-resource-group `
--location eastus `
--name your-agent-vm `
--size Standard_E4as_v4 `
--os-type linux `
--attach-os-disk your-managed-disk
```

b. *your-resource-group* Ersetzen Sie es durch den Namen der Azure Ressourcengruppe, zu der Ihr Speicherkonto gehört.

- c. ***your-agent-vm*** Ersetzen Sie es durch einen Namen für die VM, an den Sie sich erinnern können.
- d. ***your-managed-disk*** Ersetzen Sie ihn durch den Namen der verwalteten Festplatte, die Sie an die VM anhängen.
- e. Führen Sie den Befehl aus.

Sie haben Ihren Agenten bereitgestellt. Bevor Sie mit der Konfiguration Ihrer Datenübertragung beginnen können, müssen Sie den Agenten aktivieren.

Den Aktivierungsschlüssel Ihres Agenten abrufen

Gehen Sie wie folgt vor, um den Aktivierungsschlüssel Ihres DataSync Agenten manuell zu erhalten.

Alternativ [DataSync kann der Aktivierungsschlüssel automatisch für Sie abgerufen](#) werden, aber für diesen Ansatz ist eine Netzwerkkonfiguration erforderlich.

Um den Aktivierungsschlüssel Ihres Agenten zu erhalten

1. [Aktivieren Sie im Azure Portal die Startdiagnose für die VM für Ihren Agenten](#), indem Sie die Einstellung Mit benutzerdefiniertem Speicherkonto aktivieren wählen und Ihr Azure Speicherkonto angeben.

Nachdem Sie die Startdiagnose für die VM Ihres Agenten aktiviert haben, können Sie auf die lokale Konsole Ihres Agenten zugreifen, um den Aktivierungsschlüssel abzurufen.

2. Gehen Sie, während Sie sich noch im Azure Portal befinden, zu Ihrer VM und wählen Sie Serielle Konsole.
3. Melden Sie sich in der lokalen Konsole des Agenten mit den folgenden Standardanmeldedaten an:
 - Benutzername – **admin**
 - Passwort — **password**

Wir empfehlen, irgendwann mindestens das Passwort des Agenten zu ändern. Geben Sie **5** in der lokalen Konsole des Agenten das Hauptmenü ein und ändern Sie dann mit dem **passwd** Befehl das Passwort.

4. Geben Sie ein **0**, um den Aktivierungsschlüssel des Agenten zu erhalten.
5. Geben Sie den AWS-Region Ort ein, den Sie verwenden DataSync (z. B. **us-east-1**).

6. Wählen Sie den [Dienstendpunkt](#) aus, mit dem der Agent eine Verbindung herstellen soll AWS.
7. Speichern Sie den Wert der `Activation key` Ausgabe.

Ihren Agenten aktivieren

Nachdem Sie den Aktivierungsschlüssel erhalten haben, können Sie die Erstellung Ihres DataSync Agenten abschließen.

So aktivieren Sie Ihren Agenten

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich Agents und anschließend Create Agent aus.
3. Wählen Sie Microsoft Hyper-V für Hypervisor.
4. Wählen Sie als Endpunktyp den gleichen Typ von Dienstendpunkt aus, den Sie angegeben haben, als Sie den Aktivierungsschlüssel Ihres Agenten erhalten haben (wählen Sie beispielsweise Öffentliche Dienstendpunkte in **Region name**).
5. Konfigurieren Sie Ihr Netzwerk so, dass es mit dem Service-Endpunktyp funktioniert, den Ihr Agent verwendet. Informationen zu den Netzwerkanforderungen für Service-Endpunkte finden Sie in den folgenden Themen:
 - [VPC-Endpunkte](#)
 - [Öffentliche Endpunkte](#)
 - [Endpunkte für den Federal Information Processing Standard \(FIPS\)](#).
6. Gehen Sie für den Aktivierungsschlüssel wie folgt vor:
 - a. Wählen Sie Manuell geben Sie den Aktivierungsschlüssel Ihres Agenten ein.
 - b. Geben Sie den Aktivierungsschlüssel ein, den Sie von der lokalen Konsole des Agenten erhalten haben.
7. Wählen Sie Create agent (Agent erstellen) aus.

Ihr Agent ist bereit, eine Verbindung mit Ihrem herzustellen Azure Blob Storage. Weitere Informationen finden Sie unter [Erstellen Sie Ihren Azure Blob Storage Transferort](#).

EC2 Amazon-Agenten

Sie können Ihren DataSync Agenten auf einer EC2 Amazon-Instance einsetzen.

Um einen EC2 Amazon-Agenten zu erstellen

1. [Stellen Sie einen EC2 Amazon-Agenten](#) bereit.
2. [Wählen Sie einen Service-Endpunkt](#), mit dem der Agent kommuniziert AWS.

In diesem Fall empfehlen wir die Verwendung eines Virtual Private Cloud (VPC) - Dienstendpunkts.

3. Konfigurieren Sie Ihr Netzwerk so, dass es mit [VPC-Dienstendpunkten](#) funktioniert.
4. [Aktivieren Sie den Agenten](#).

Erstellen Sie Ihren Azure Blob Storage Transferort

Sie können so konfigurieren DataSync , dass Sie Azure Blob Storage als Übertragungsquelle oder -ziel verwendet werden.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie wissen, [wie auf DataSync Zugriffsebenen Azure Blob Storage und Blob-Typen zugegriffen](#) wird und wie mit ihnen gearbeitet wird. Sie benötigen außerdem einen [DataSync Agenten](#), der eine Verbindung zu Ihrem Azure Blob Storage Container herstellen kann.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie für Speichertyp die Option Microsoft Azure Blob Storage aus.
4. Geben Sie unter Container-URL die URL des Containers ein, der an Ihrer Übertragung beteiligt ist.
5. (Optional) Wählen Sie unter Zugriffsebene bei Verwendung als Ziel die [Zugriffsebene](#) aus, in die Ihre Objekte oder Dateien übertragen werden sollen.
6. Geben Sie unter Ordner Pfadsegmente ein, wenn Sie die Übertragung auf ein virtuelles Verzeichnis in Ihrem Container beschränken möchten (z. B. /my/images).
7. Wenn für Ihre Übertragung ein Agent erforderlich ist, wählen Sie Agenten verwenden und dann den DataSync Agenten aus, der eine Verbindung zu Ihrem Azure Blob Storage Container herstellen kann.

8. Geben Sie für das SAS-Token die Anmeldeinformationen ein, die für den DataSync Zugriff auf Ihren Blob-Speicher erforderlich sind. Für einige öffentliche Datensätze im Azure Blob Storage sind keine Anmeldeinformationen erforderlich. Sie können ein SAS-Token direkt eingeben oder ein AWS Secrets Manager Geheimnis angeben, das das Token enthält. Weitere Informationen finden Sie unter [Bereitstellen von Anmeldeinformationen für Speicherorte](#).

Ihr SAS-Token ist Teil der SAS-URI-Zeichenfolge, die nach Ihrer Speicherressourcen-URI und einem Fragezeichen (?) steht. Ein Token sieht ungefähr so aus:

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=aBBKD%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

9. (Optional) Geben Sie Werte für die Felder Schlüssel und Wert ein, um den Standort zu kennzeichnen.

Mithilfe von Stichwörtern können Sie Ihre AWS Ressourcen verwalten, filtern und nach ihnen suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

10. Wählen Sie Standort erstellen aus.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden `create-location-azure-blob` Befehl:

```
aws datasync create-location-azure-blob \
  --container-url "https://path/to/container" \
  --authentication-type "SAS" \
  --sas-configuration '{
    "Token": "your-sas-token"
  }' \
  --agent-arns my-datasync-agent-arn \
  --subdirectory "/path/to/my/data" \
  --access-tier "access-tier-for-destination" \
  --tags [{"Key": "key1", "Value": "value1"}]
```

2. Geben Sie für den `--container-url` Parameter die URL des Azure Blob Storage Containers an, der an Ihrer Übertragung beteiligt ist.
3. Geben Sie für den Parameter `--authentication-type` SAS an: Wenn Sie auf einen öffentlichen Datensatz zugreifen, für den keine Authentifizierung erforderlich ist, geben Sie Folgendes an NONE.

4. Geben Sie für die Token Option des `--sas-configuration` Parameters das SAS-Token an, das den DataSync Zugriff auf Ihren Blob-Speicher ermöglicht.

Sie können auch zusätzliche Parameter für die Sicherung Ihrer Schlüssel mithilfe von AWS Secrets Manager angeben. Weitere Informationen finden Sie unter [Bereitstellen von Anmeldeinformationen für Speicherorte](#).

Ihr SAS-Token ist Teil der SAS-URI-Zeichenfolge, die nach Ihrer Speicherressourcen-URI und einem Fragezeichen (?) steht. Ein Token sieht ungefähr so aus:

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=aBBKD%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

5. (Optional) Geben Sie für den `--agent-arns` Parameter den Amazon-Ressourcennamen (ARN) des DataSync Agenten an, der eine Verbindung zu Ihrem Container herstellen kann.

Hier ist ein Beispiel für einen Agenten-ARN: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

Sie können mehr als einen Agenten angeben. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

6. Geben Sie für den `--subdirectory` Parameter Pfadsegmente an, wenn Sie Ihre Übertragung auf ein virtuelles Verzeichnis in Ihrem Container beschränken möchten (z. B. `/my/images`).
7. (Optional) Geben Sie für den `--access-tier` Parameter die [Zugriffsebene](#) (HOTC00L, oder ARCHIVE) an, in die Ihre Objekte oder Dateien übertragen werden sollen.

Dieser Parameter gilt nur, wenn Sie diesen Speicherort als Übertragungsziel verwenden.

8. (Optional) Geben Sie für den `--tags` Parameter Schlüssel-Wert-Paare an, die Ihnen bei der Verwaltung, Filterung und Suche nach Ihrem Standort helfen können.

Wir empfehlen, ein Namensschild für Ihren Standort zu erstellen.

9. Führen Sie den Befehl `create-location-azure-blob` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN des Speicherorts anzeigt, den Sie erstellt haben. Zum Beispiel:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh"
```

```
}
```

Ihr Azure Blob Storage Übertragungsort wird angezeigt

Sie können Details zum bestehenden DataSync Transferort für Sie abrufen Azure Blob Storage.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
3. Wählen Sie Ihren Azure Blob Storage Standort aus.

Sie können Details zu Ihrem Standort einsehen, einschließlich aller DataSync Übertragungsaufgaben, für die dieser Standort verwendet wird.

Mit dem AWS CLI

1. Kopieren Sie den folgenden `describe-location-azure-blob` Befehl:

```
aws datasync describe-location-azure-blob \
  --location-arn "your-azure-blob-location-arn"
```

2. Geben Sie für den `--location-arn` Parameter den ARN für den Azure Blob Storage Speicherort an, den Sie erstellt haben (z. B. `arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Führen Sie den Befehl `describe-location-azure-blob` aus.

Sie erhalten eine Antwort, die Ihnen Details zu Ihrem Standort zeigt. Zum Beispiel:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh",
  "LocationUri": "azure-blob://my-user.blob.core.windows.net/container-1",
  "AuthenticationType": "SAS",
  "Subdirectory": "/my/images",
  "AgentArns": ["arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890deadfb"],
}
```

Aktualisierung Ihres Azure Blob Storage Übertragungsorts

Bei Bedarf können Sie die Konfiguration Ihres Standorts in der Konsole oder mithilfe der ändern AWS CLI.

Mit dem AWS CLI

1. Kopieren Sie den folgenden `update-location-azure-blob` Befehl:

```
aws datasync update-location-azure-blob \
  --location-arn "your-azure-blob-location-arn" \
  --authentication-type "SAS" \
  --sas-configuration '{
    "Token": "your-sas-token"
  }' \
  --agent-arns my-datasync-agent-arn \
  --subdirectory "/path/to/my/data" \
  --access-tier "access-tier-for-destination"
```

2. Geben Sie für den `--location-arn` Parameter den ARN für den Azure Blob Storage Standort an, den Sie aktualisieren (z. B. `arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Geben Sie für den Parameter `--authentication-type` SAS an:
4. Geben Sie für die Token Option des `--sas-configuration` Parameters das SAS-Token an, das den DataSync Zugriff auf Ihren Blob-Speicher ermöglicht.

Das Token ist Teil der SAS-URI-Zeichenfolge, die nach dem Speicherressourcen-URI und einem Fragezeichen (?) steht. Ein Token sieht ungefähr so aus:

```
sp=r&st=2022-12-20T14:54:52Z&se=2022-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=qCBKD%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

5. Geben Sie für den `--agent-arns` Parameter den Amazon-Ressourcennamen (ARN) des DataSync Agenten an, den Sie mit Ihrem Container verbinden möchten.

Hier ist ein Beispiel für einen Agenten-ARN: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

Sie können mehr als einen Agenten angeben. Weitere Informationen finden Sie unter [Verwendung mehrerer DataSync Agenten](#).

6. Geben Sie für den `--subdirectory` Parameter Pfadsegmente an, wenn Sie Ihre Übertragung auf ein virtuelles Verzeichnis in Ihrem Container beschränken möchten (z. B. `/my/images`).
7. (Optional) Geben Sie für den `--access-tier` Parameter die [Zugriffsebene](#) (HOTCOOL, oder ARCHIVE) an, in die Ihre Objekte übertragen werden sollen.

Dieser Parameter gilt nur, wenn Sie diesen Standort als Übertragungsziel verwenden.

Nächste Schritte

Nachdem Sie mit der Erstellung eines DataSync Standorts für Ihren fertig sind Azure Blob Storage, können Sie mit der Einrichtung Ihres Transfers fortfahren. Hier sind einige der nächsten Schritte, die Sie berücksichtigen sollten:

1. Falls Sie dies noch nicht getan haben, [erstellen Sie einen anderen Speicherort](#), an den Sie Ihre Daten übertragen möchten oder von Ihrem Azure Blob Storage.
2. Erfahren Sie, DataSync [wie mit Metadaten und speziellen Dateien](#) umgegangen wird, insbesondere wenn Ihre Übertragungsorte keine ähnliche Metadatenstruktur haben.
3. Konfigurieren Sie, wie Ihre Daten übertragen werden. Sie können beispielsweise [nur einen Teil Ihrer Daten übertragen oder Dateien in Ihrem](#) Blob-Speicher löschen, die sich nicht an Ihrem Quellspeicherort befinden (sofern Ihr [SAS-Token](#) über Löschberechtigungen verfügt).
4. [Starten Sie Ihre Übertragung](#).

AWS DataSync Transfers konfigurieren mit Microsoft Azure Files SMB-Aktien

Sie können so konfigurieren AWS DataSync , dass Daten zu oder von einem übertragen werden Microsoft Azure Files SMB-Freigabe (Server Message Block).

Tip

[Eine vollständige Anleitung zum Verschieben von Daten aus Azure Files SMB-Shares zu finden Sie im AWS Storage-Blog.](#)

Bereitstellung des DataSync Zugriffs auf SMB-Shares

DataSync stellt über das SMB-Protokoll eine Verbindung zu Ihrem SMB-Share her und authentifiziert sich mit den von Ihnen angegebenen Anmeldeinformationen.

Themen

- [Unterstützte SMB-Protokollversionen](#)
- [Erforderliche Berechtigungen](#)

Unterstützte SMB-Protokollversionen

Wählt standardmäßig DataSync automatisch eine Version des SMB-Protokolls auf der Grundlage der Verhandlungen mit Ihrem SMB-Dateiserver aus.

Sie können auch die Verwendung einer bestimmten SMB-Version konfigurieren. Wir empfehlen jedoch, dies nur dann DataSync zu tun, wenn DataSync Probleme bei der automatischen Aushandlung mit dem SMB-Dateiserver auftreten. DataSync unterstützt SMB-Versionen 1.0 und höher. Aus Sicherheitsgründen empfehlen wir die Verwendung von SMB Version 3.0.2 oder höher. Frühere Versionen, wie SMB 1.0, enthalten bekannte Sicherheitslücken, die Angreifer ausnutzen können, um Ihre Daten zu gefährden.

In der folgenden Tabelle finden Sie eine Liste der Optionen in der DataSync Konsole und der API:

Konsolenoption	API-Option	Beschreibung
Automatisch	AUTOMATIC	DataSync und der SMB-Dateiserver handeln zwischen 2.1 und 3.1.1 die höchste Version von SMB aus, die sie gegenseitig unterstützen. Dies ist die Standardoption und wird empfohlen. Wenn Sie stattdessen eine bestimmte Version auswählen, die Ihr Dateiserver nicht unterstützt, erhalten Sie möglicherweise eine Operation Not Supported -Fehlermeldung.
SMB 3.0.2	SMB3	Beschränkt die Protokollaushandlung nur auf SMB-Version 3.0.2.

Konsolenoption	API-Option	Beschreibung
SMB 2.1	SMB2	Beschränkt die Protokollaushandlung nur auf SMB-Version 2.1.
SMB 2.0	SMB2_0	Beschränkt die Protokollaushandlung nur auf SMB Version 2.0.
SMB 1.0	SMB1	Beschränkt die Protokollaushandlung nur auf SMB Version 1.0.

Erforderliche Berechtigungen

DataSync benötigt einen Benutzer, der berechtigt ist, Ihren SMB-Standort bereitzustellen und darauf zuzugreifen. Dies kann ein lokaler Benutzer auf Ihrem Windows-Dateiserver oder ein Domänenbenutzer sein, der in Ihrem Microsoft Active Directory definiert ist.

Um den Objekteigentum festzulegen, ist die SE_RESTORE_NAME Berechtigung DataSync erforderlich, die normalerweise Mitgliedern der integrierten Active Directory-Gruppen Backup-Operatoren und Domänenadministratoren gewährt wird. Wenn Sie einem Benutzer dieses Recht gewähren, können Sie auch sicherstellen, dass ausreichende Berechtigungen für Dateien, Ordner und Dateimetadaten vorhanden sind, mit Ausnahme von NTFS-Systemzugriffskontrolllisten (SACLs). DataSync

Zum Kopieren SACLs sind zusätzliche Rechte erforderlich. Dazu ist insbesondere das SE_SECURITY_NAME Windows-Recht erforderlich, das Mitgliedern der Gruppe Domänen-Admins gewährt wird. Wenn Sie Ihre Aufgabe für das Kopieren konfigurieren SACLs, stellen Sie sicher, dass der Benutzer über die erforderlichen Rechte verfügt. Weitere Informationen zur Konfiguration einer Aufgabe zum Kopieren SACLs finden Sie unter [Konfiguration des Umgangs mit Dateien, Objekten und Metadaten](#).

Wenn Sie Daten zwischen einem SMB-Dateiserver und dem Dateisystem Amazon FSx for Windows File Server kopieren, müssen Quell- und Zielspeicherorte derselben Microsoft Active Directory-Domäne angehören oder eine Active Directory-Vertrauensstellung zwischen ihren Domänen bestehen.

Erstellen Sie Ihren Azure Files-Übertragungsort mithilfe der Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.

2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie für Location type (Speicherorttyp) Server Message Block (SMB).

Sie konfigurieren diesen Speicherort später als Quelle oder Ziel.

4. Wählen Sie unter Agenten einen oder mehrere DataSync Agenten aus, die Sie mit Ihrem SMB-Share verbinden möchten.

Wenn Sie mehr als einen Agenten auswählen, stellen Sie sicher, dass Sie verstehen, [mehrere Agenten für einen Standort](#) zu verwenden.

5. Geben Sie für SMB-Server den DNS-Namen (Domain Name System) oder die IP-Adresse der SMB-Freigabe ein, die Ihr DataSync Agent bereitstellen wird.

 Note

Sie können keine IP-Adresse der Version 6 (IPv6) angeben.

6. Geben Sie unter Freigabename den Namen der Freigabe ein, die von Ihrer SMB-Freigabe exportiert wurde und in die Daten gelesen oder geschrieben DataSync werden sollen.

Sie können ein Unterverzeichnis in den Freigabepfad aufnehmen (z. B. /path/to/subdirectory). Stellen Sie sicher, dass andere SMB-Clients in Ihrem Netzwerk diesen Pfad ebenfalls bereitstellen können.

Um alle Daten im Unterverzeichnis zu kopieren, DataSync müssen Sie in der Lage sein, die SMB-Freigabe zu mounten und auf alle zugehörigen Daten zuzugreifen. Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

7. (Optional) Erweitern Sie Zusätzliche Einstellungen und wählen Sie eine SMB-Version aus, die Sie beim Zugriff auf Ihre SMB-Freigabe verwenden möchten. DataSync

Wählt standardmäßig DataSync automatisch eine Version aus, die auf Verhandlungen mit der SMB-Aktie basiert. Weitere Informationen finden Sie unter [Unterstützte SMB-Versionen](#).

8. Geben Sie unter Benutzer einen Benutzernamen ein, der Ihre SMB-Freigabe bereitstellen kann und über Zugriffsrechte auf die Dateien und Ordner verfügt, die an Ihrer Übertragung beteiligt sind.

Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).

9. Geben Sie unter Passwort das Passwort des Benutzers ein, der Ihre SMB-Freigabe bereitstellen kann und berechtigt ist, auf die Dateien und Ordner zuzugreifen, die an Ihrer Übertragung beteiligt sind.
10. (Optional) Geben Sie unter Domain den Windows-Domänennamen ein, zu dem Ihre SMB-Freigabe gehört.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieser Einstellung sichergestellt, dass DataSync eine Verbindung zur richtigen Freigabe hergestellt wird.

11. (Optional) Wählen Sie Tag hinzufügen, um Ihren Standort zu taggen.

Stichwörter sind Schlüssel-Wert-Paare, die dir helfen, deine Standorte zu verwalten, zu filtern und nach ihnen zu suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

12. Wählen Sie Standort erstellen aus.

Konfiguration von Übertragungen mit anderem Cloud-Objektspeicher

Mit AWS DataSync können Sie Daten zwischen [AWS Speicherdiensten](#) und den folgenden Cloud-Objektspeicheranbietern übertragen:

- [Wasabi Cloud Storage](#)
- [DigitalOcean Spaces](#)
- [Oracle Cloud Infrastructure Object Storage](#)
- [Cloudflare R2 Storage](#)
- [Backblaze B2 Cloud Storage](#)
- [NAVER Cloud Object Storage](#)
- [Alibaba Cloud Object Storage Service](#)
- [IBM Cloud Object Storage](#)
- [Seagate Lyve Cloud](#)

Ein DataSync Agent ist nur erforderlich, wenn Daten zwischen Speichersystemen in anderen Clouds und Amazon EFS oder Amazon FSx übertragen werden oder wenn Aufgaben im Basismodus verwendet werden. Sie benötigen keinen Agenten, um Daten zwischen Speichersystemen in anderen Clouds und Amazon S3 im erweiterten Modus zu übertragen.

Unabhängig davon, ob Sie einen Agenten verwenden, müssen Sie auch einen [Übertragungsort](#) für Ihren Cloud-Objektspeicher (insbesondere einen Objektspeicherort) erstellen. DataSync kann diesen Speicherort als Quelle oder Ziel für Ihre Übertragung verwenden.

Bereitstellung des DataSync Zugriffs auf Ihren anderen Cloud-Objektspeicher

Wie auf Ihren Cloud-Objektspeicher DataSync zugegriffen wird, hängt von mehreren Faktoren ab, unter anderem davon, ob Ihr Speicher mit der Amazon S3 S3-API kompatibel ist und von den Berechtigungen und Anmeldeinformationen, die DataSync für den Zugriff auf Ihren Speicher erforderlich sind.

Themen

- [Amazon S3 S3-API-Kompatibilität](#)
- [Speicherberechtigungen und Endpunkte](#)
- [Anmeldeinformationen für den Speicher](#)

Amazon S3 S3-API-Kompatibilität

Ihr Cloud-Objektspeicher muss mit den folgenden [Amazon S3 S3-API-Vorgängen](#) kompatibel sein, DataSync um eine Verbindung zu ihm herstellen zu können:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetBucketLocation
- GetObject
- GetObjectTagging
- HeadBucket
- HeadObject
- ListObjectsV2

- PutObject
- PutObjectTagging
- UploadPart

Speicherberechtigungen und Endpunkte

Sie müssen die Berechtigungen konfigurieren, die den DataSync Zugriff auf Ihren Cloud-Objektspeicher ermöglichen. Wenn es sich bei Ihrem Objektspeicher um einen Quellspeicherort handelt, DataSync sind Lese- und Listenberechtigungen für den Bucket erforderlich, aus dem Sie Daten übertragen. Wenn es sich bei Ihrem Objektspeicher um einen Zielspeicherort handelt, DataSync benötigt er Lese-, Listen-, Schreib- und Löschberechtigungen für den Bucket.

DataSync benötigt außerdem einen Endpunkt (oder Server), um eine Verbindung zu Ihrem Speicher herzustellen. In der folgenden Tabelle werden die Endpunkte beschrieben, die für den Zugriff auf andere Cloud-Objektspeicher verwendet werden DataSync können:

Anderer Cloud-Anbieter	Endpunkt
Wasabi Cloud Storage	S3. <i>region</i> .wasabisys.com
DigitalOcean Spaces	<i>region</i> .digitaloceanspaces.com
Oracle Cloud Infrastructure Object Storage	<i>namespace</i> .compat.objectstorage. <i>region</i> .oraclecloud.com
Cloudflare R2 Storage	<i>account-id</i> .r2.cloudflarestorage.com
Backblaze B2 Cloud Storage	S3. <i>region</i> .backblazeb2.com
NAVER Cloud Object Storage	<i>region</i> .object.ncloudstorage.com (die meisten Regionen)
Alibaba Cloud Object Storage Service	<i>region</i> .aliyuncs.com
IBM Cloud Object Storage	s3. <i>region</i> .cloud-object-storage.appdomain.cloud
Seagate Lyve Cloud	s3. <i>region</i> .lyvecloud.seagate.com

 Important

Einzelheiten zur Konfiguration von Bucket-Berechtigungen und aktualisierte Informationen zu Speicherendpunkten finden Sie in der Dokumentation Ihres Cloud-Anbieters.

Anmeldeinformationen für den Speicher

DataSync benötigt außerdem die Anmeldeinformationen für den Zugriff auf den Objektspeicher-Bucket, der an Ihrer Übertragung beteiligt ist. Dies kann ein Zugriffsschlüssel und ein geheimer Schlüssel oder etwas Ähnliches sein, je nachdem, wie Ihr Cloud-Speicheranbieter auf diese Anmeldeinformationen verweist.

Weitere Informationen finden Sie in der Dokumentation Ihres Cloud-Anbieters.

Überlegungen bei der Übertragung von einem anderen Cloud-Objektspeicher

Wenn Sie planen, Objekte mithilfe von Cloud Storage zu oder von einem anderen Cloud-Speicheranbieter zu übertragen DataSync, sollten Sie einige Dinge beachten.

Themen

- [Kosten](#)
- [Speicherklassen](#)
- [Objekt-Tags](#)
- [Übertragung auf Amazon S3](#)

Kosten

Die Gebühren, die mit dem Verschieben von Daten zu und von einem anderen Cloud-Speicheranbieter verbunden sind, können Folgendes beinhalten:

- Eine [EC2Amazon-Instance](#) für Ihren DataSync Agenten ausführen
- Übertragung der Daten mithilfe von Amazon S3 [DataSync](#), einschließlich Anforderungsgebühren im Zusammenhang mit Ihrem Cloud-Objektspeicher und [Amazon S3](#) (wenn S3 Ihr Übertragungsziel ist)
- Übertragung von Daten in oder aus Ihrem Cloud-Speicher (überprüfen Sie die Preise Ihres Cloud-Anbieters)

- Speichern von Daten in einem [AWS Speicherdienst](#), der unterstützt wird von DataSync
- Speichern von Daten bei einem anderen Cloud-Anbieter (überprüfen Sie die Preise Ihres Cloud-Anbieters)

Speicherklassen

Einige Cloud-Speicheranbieter haben Speicherklassen (ähnlich wie [Amazon S3](#)), die nicht gelesen werden DataSync können, ohne zuvor wiederhergestellt zu werden. Oracle Cloud Infrastructure Object Storage hat beispielsweise eine Archivspeicherklasse. Sie müssen Objekte in dieser Speicherklasse wiederherstellen, bevor DataSync Sie sie übertragen können. Weitere Informationen finden Sie in der Dokumentation Ihres Cloud-Anbieters.

Objekt-Tags

Nicht alle Cloud-Anbieter unterstützen Objekt-Tags. Diejenigen, die dies tun, erlauben möglicherweise nicht, Tags über die Amazon S3 S3-API abzufragen. In beiden Situationen schlägt Ihre DataSync Übertragungsaufgabe möglicherweise fehl, wenn Sie versuchen, Objekt-Tags zu kopieren.

Sie können dies vermeiden, indem Sie das Kontrollkästchen Objekt-Tags kopieren in der DataSync Konsole deaktivieren, wenn Sie Ihre Aufgabe erstellen, starten oder aktualisieren.

Übertragung auf Amazon S3

Bei der Übertragung auf Amazon S3 DataSync können keine Objekte übertragen werden, die größer als 5 TB sind. DataSync kann auch nur Objektmetadaten mit einer Größe von bis zu 2 KB kopieren.

Erstellen Sie Ihren DataSync Agenten

Ein DataSync Agent ist nur erforderlich, wenn Daten zwischen Speichersystemen in anderen Clouds und Amazon EFS oder Amazon FSx übertragen werden oder wenn Aufgaben im Basismodus verwendet werden. Sie benötigen keinen Agenten, um Daten zwischen Speichersystemen in anderen Clouds und Amazon S3 im erweiterten Modus zu übertragen. In diesem Abschnitt wird beschrieben, wie Sie einen Agenten auf einer EC2 Amazon-Instance in Ihrer Virtual Private Cloud (VPC) bereitstellen und aktivieren. AWS

Um einen EC2 Amazon-Agenten zu erstellen

1. [Stellen Sie einen EC2 Amazon-Agenten](#) bereit.

2. [Wählen Sie einen Service-Endpunkt](#), mit dem der Agent kommuniziert AWS.

In diesem Fall empfehlen wir die Verwendung eines VPC-Dienstendpunkts.

3. Konfigurieren Sie Ihr Netzwerk so, dass es mit [VPC-Dienstendpunkten](#) funktioniert.
4. [Aktivieren Sie den Agenten](#).

Erstellen Sie einen Übertragungsort für Ihren anderen Cloud-Objektspeicher

Sie können so konfigurieren DataSync, dass Ihr Cloud-Objektspeicher als Quell- oder Zielort verwendet wird.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie wissen, [wie DataSync auf Ihren Cloud-Objektspeicher zugegriffen wird](#). Sie benötigen außerdem einen [DataSync Agenten](#), der eine Verbindung zu Ihrem Cloud-Objektspeicher herstellen kann.

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte und Standort erstellen aus.
3. Wählen Sie als Standorttyp die Option Objektspeicher aus.
4. Geben Sie für Server den [Endpunkt](#) ein, über den Sie auf Ihren Cloud-Objektspeicher zugreifen DataSync können:
 - Wasabi Cloud Storage – `S3.region.wasabisys.com`
 - DigitalOcean Spaces – `region.digitaloceanspaces.com`
 - Oracle Cloud Infrastructure Object Storage –
`namespace.compat.objectstorage.region.oraclecloud.com`
 - Cloudflare R2 Storage – `account-id.r2.cloudflarestorage.com`
 - Backblaze B2 Cloud Storage – `S3.region.backblazeb2.com`
 - NAVER Cloud Object Storage— `region.object.ncloudstorage.com` (die meisten Regionen)
 - Alibaba Cloud Object Storage Service – `region.aliyuncs.com`
 - IBM Cloud Object Storage – `s3.region.cloud-object-storage.appdomain.cloud`
 - Seagate Lyve Cloud – `s3.region.lyvecloud.seagate.com`

5. Geben Sie als Bucket-Namen den Namen des Object-Storage-Buckets ein, zu dem Sie Daten übertragen oder von dem Sie Daten übertragen.
6. Geben Sie für Ordner ein Objektpräfix ein. DataSync überträgt nur Objekte mit diesem Präfix.
7. Wenn für Ihre Übertragung ein Agent erforderlich ist, wählen Sie Agenten verwenden und dann den DataSync Agenten aus, der eine Verbindung zu Ihrem Cloud-Objektspeicher herstellen kann.
8. Erweitern Sie Additional settings (Zusätzliche Einstellungen). Wählen Sie als Serverprotokoll HTTPS aus. Wählen Sie 443 für Serverport aus.
9. Scrollen Sie nach unten zum Abschnitt Authentifizierung. Vergewissern Sie sich, dass das Kontrollkästchen Anmeldeinformationen erforderlich aktiviert ist, und geben Sie dann DataSync Ihre [Speicheranmeldedaten ein](#).
 - Geben Sie unter Zugriffsschlüssel die ID für den Zugriff auf Ihren Cloud-Objektspeicher ein.
 - Geben Sie unter Geheimer Schlüssel den geheimen Schlüssel für den Zugriff auf Ihren Cloud-Objektspeicher ein. Sie können den Schlüssel entweder direkt eingeben oder ein AWS Secrets Manager Geheimnis angeben, das den Schlüssel enthält. Weitere Informationen finden Sie unter [Bereitstellen von Anmeldeinformationen für Speicherorte](#).
10. (Optional) Geben Sie Werte für die Felder Schlüssel und Wert ein, um den Speicherort zu kennzeichnen.

Mithilfe von Stichwörtern können Sie Ihre AWS Ressourcen verwalten, filtern und nach ihnen suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.
11. Wählen Sie Standort erstellen aus.

Nächste Schritte

Nachdem Sie mit der Erstellung eines DataSync Speicherorts für Ihren Cloud-Objektspeicher fertig sind, können Sie mit der Einrichtung Ihrer Übertragung fortfahren. Hier sind einige der nächsten Schritte, die Sie berücksichtigen sollten:

1. Falls Sie dies noch nicht getan haben, [erstellen Sie einen anderen Speicherort](#), an den Sie Ihre Daten übertragen möchten oder von dort aus AWS.
2. Erfahren Sie, DataSync [wie mit Metadaten und speziellen Dateien](#) für Objektspeicherorte umgegangen wird.
3. Konfigurieren Sie, wie Ihre Daten übertragen werden. Vielleicht möchten Sie beispielsweise nur [eine Teilmenge Ihrer Daten übertragen](#).

 Important

Stellen Sie sicher, dass Sie konfigurieren, wie Objekt-Tags korrekt DataSync kopiert werden. Weitere Informationen finden Sie unter Überlegungen zu [Objekt-Tags](#).

4. [Starte deine Übertragung](#).

Eine Aufgabe für die Übertragung Ihrer Daten erstellen

Eine Aufgabe beschreibt, wo und wie Daten AWS DataSync übertragen werden. Eine Aufgabe besteht aus den folgenden Komponenten:

- [Quellstandort](#) — Das Speichersystem oder der Dienst, von dem Daten DataSync übertragen werden.
- [Zielort](#) — Das Speichersystem oder der Dienst, zu dem Daten DataSync übertragen werden.
- [Aufgabenoptionen](#) — Einstellungen, z. B. welche Dateien übertragen werden sollen, wie Daten verifiziert werden, wann die Aufgabe ausgeführt wird und vieles mehr.
- [Aufgabenausführungen](#) — Wenn Sie eine Aufgabe ausführen, wird dies als Aufgabenausführung bezeichnet.

Ihre Aufgabe erstellen

Wenn Sie eine DataSync Aufgabe erstellen, geben Sie Ihre Quell- und Zielorte an. Sie können Ihre Aufgabe auch anpassen, indem Sie auswählen, welche Dateien übertragen werden sollen, wie Metadaten behandelt werden, einen Zeitplan einrichten und vieles mehr.

Bevor Sie Ihre Aufgabe erstellen, sollten Sie sicherstellen, dass Sie wissen, [wie DataSync Übertragungen funktionieren](#), und überprüfen Sie die [Aufgabenkontingente](#).

 Important

Wenn Sie planen, Daten zu oder von einem Amazon S3 S3-Standort zu übertragen, lesen Sie zunächst, [wie sich dies auf Ihre S3-Anforderungsgebühren auswirken DataSync kann](#), sowie auf der [DataSync Preisseite](#).

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Stellen Sie sicher, dass Sie sich in einem der Länder AWS-Regionen befinden, in die Sie Daten übertragen möchten.
3. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und dann Aufgabe erstellen aus.
4. [Erstellen](#) oder wählen Sie auf der Seite Quellspeicherort konfigurieren einen Quellspeicherort aus und klicken Sie dann auf Weiter.
5. [Erstellen](#) oder wählen Sie auf der Seite Zielort konfigurieren einen Zielstandort aus und klicken Sie dann auf Weiter.
6. (Empfohlen) Geben Sie Ihrer Aufgabe auf der Seite „Einstellungen konfigurieren“ einen Namen, den Sie sich merken können.
7. Wählen Sie auf der Seite „Einstellungen konfigurieren“ Ihre Aufgabenoptionen aus oder verwenden Sie die Standardeinstellungen.

Einige der folgenden Optionen könnten Sie interessieren:

- Geben Sie den [Aufgabenmodus](#) an, den Sie verwenden möchten.
- Geben Sie mithilfe eines [Manifests](#) oder von [Filtern](#) an, welche Daten übertragen werden sollen.
- Konfigurieren Sie, wie [Dateimetadaten behandelt](#) werden sollen, und [überprüfen Sie die Datenintegrität](#).
- Überwachen Sie Ihre Übertragung mit [Aufgabenberichten](#) oder [Amazon CloudWatch](#). Wir empfehlen, eine Art Überwachung für Ihre Aufgabe einzurichten.

Wählen Sie abschließend Weiter.

8. Überprüfen Sie Ihre Aufgabenkonfiguration und wählen Sie dann Aufgabe erstellen.

Sie sind bereit, [Ihre Aufgabe zu starten](#).

Mit dem AWS CLI

Sobald Sie [Ihre DataSync Quell- und Zielspeicherorte erstellt](#) haben, können Sie Ihre Aufgabe erstellen.

1. Stellen Sie in Ihren AWS CLI Einstellungen sicher, dass Sie einen der Orte verwenden AWS-Regionen , an die Sie Daten übertragen möchten.
2. Kopieren Sie den folgenden create-task Befehl:

```
aws datasync create-task \  
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --name "task-name"
```

3. Geben Sie für --source-location-arn den Amazon-Ressourcennamen (ARN) Ihres Quellstandorts an.
4. Geben Sie für --destination-location-arn den ARN Ihres Zielstandorts an.

Wenn du zwischen AWS-Regionen unseren Konten überweist, vergewissere dich, dass der ARN die andere Region oder Konto-ID enthält.

5. (Empfohlen) Geben Sie für --name einen Namen für Ihre Aufgabe an, an den Sie sich erinnern können.
6. Geben Sie nach Bedarf weitere Aufgabenoptionen an. Einige der folgenden Optionen könnten Sie interessieren:
 - Geben Sie mithilfe eines [Manifests](#) oder von [Filtern](#) an, welche Daten übertragen werden sollen.
 - Konfigurieren Sie, wie [Dateimetadaten behandelt](#) werden sollen, und [überprüfen Sie die Datenintegrität](#).
 - Überwachen Sie Ihre Übertragung mit [Aufgabenberichten](#) oder [Amazon CloudWatch](#). Wir empfehlen, eine Art Überwachung für Ihre Aufgabe einzurichten.

Weitere Optionen finden Sie unter [create-task](#). Hier ist ein create-task Beispielfehl, der mehrere Optionen angibt:

```
aws datasync create-task \  
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --cloud-watch-log-group-arn "arn:aws:logs:region:account-id" \  
  --name "task-name"
```

```
--name "task-name" \  
--options  
VerifyMode=NONE,OverwriteMode=NEVER,Atime=BEST_EFFORT,Mtime=PRESERVE,Uid=INT_VALUE,Gid=INT
```

7. Führen Sie den Befehl `create-task` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN der Aufgabe anzeigt, die Sie erstellt haben. Beispiel:

```
{  
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/  
task-08de6e6697796f026"  
}
```

Sie sind bereit, [Ihre Aufgabe zu starten](#).

Status der Aufgaben

Wenn Sie eine DataSync Aufgabe erstellen, können Sie ihren Status überprüfen, um festzustellen, ob sie zur Ausführung bereit ist.

Status der Konsole	API-Status	Description
Available (Verfügbar)	AVAILABLE	Die Aufgabe ist bereit, mit der Übertragung von Daten zu beginnen.
In Ausführung	RUNNING	Eine Aufgabenausführung ist im Gange. Weitere Informationen finden Sie unter Status der Aufgabenausführung .
Nicht verfügbar	UNAVAILABLE	Ein von der Aufgabe verwendeter DataSync Agent ist offline. Weitere Informationen finden Sie unter Was mache ich, wenn mein Agent offline ist? .
In Warteschlange eingefügt	QUEUED	Eine weitere Aufgabenausführung, die denselben DataSync Agenten verwendet, ist im Gange. Weitere Informationen finden Sie unter Wissen Sie, wann sich Ihre Aufgabe in der Warteschlange befindet .

Partitionierung großer Datensätze mit mehreren Aufgaben

Wenn Sie einen großen Datensatz übertragen, z. B. Millionen von Dateien oder Objekten [migrieren](#), empfehlen wir, für Ihre Übertragung den DataSync erweiterten Modus zu verwenden, mit dem Datensätze mit praktisch unbegrenzter Anzahl von Dateien übertragen werden können. Bei sehr großen Datensätzen mit Milliarden von Dateien sollten Sie erwägen, Ihren Datensatz mit mehreren Aufgaben zu partitionieren. DataSync Die Partitionierung Ihrer Daten auf mehrere Aufgaben (und möglicherweise auf [Agenten](#), je nach Standort) trägt dazu bei, den Zeitaufwand für die Vorbereitung und Übertragung Ihrer Daten DataSync zu reduzieren.

Überlegen Sie sich einige Möglichkeiten, wie Sie einen großen Datensatz auf mehrere DataSync Aufgaben partitionieren können:

- Erstellen Sie Aufgaben, die separate Ordner übertragen. Sie könnten beispielsweise zwei Aufgaben erstellen, die auf Ihren Quellspeicher abzielen `/FolderA` und `/FolderB` sich dort befinden.
- Erstellen Sie Aufgaben, die mithilfe eines [Manifests](#) oder von [Filtern](#) Teilmengen von Dateien, Objekten und Ordnern übertragen.

Beachten Sie, dass dieser Ansatz die Auslastung Ihres Speichers I/O erhöhen und sich auf Ihre Netzwerkbandbreite auswirken kann. Weitere Informationen finden Sie im Blog [So beschleunigen Sie Ihre Datenübertragungen mit DataSync Scale-out-Architekturen](#).

Segmentierung übertragener Daten mit mehreren Aufgaben

Wenn Sie verschiedene Datensätze an dasselbe Ziel übertragen, können Sie mehrere Aufgaben erstellen, um die zu übertragenden Daten zu segmentieren.

Wenn Sie beispielsweise in denselben S3-Bucket mit dem Namen `übertragenMyBucket`, können Sie im Bucket unterschiedliche Präfixe erstellen, die jeder Aufgabe entsprechen. Dieser Ansatz verhindert Dateinamenkonflikte zwischen den Datensätzen und ermöglicht es Ihnen, für jedes Präfix unterschiedliche Berechtigungen festzulegen. So könnten Sie das einrichten:

1. Erstellen Sie drei Präfixe im Ziel `MyBucket` mit den Namen `task1`, `task2`, und `task3`:
 - `s3://MyBucket/task1`
 - `s3://MyBucket/task2`
 - `s3://MyBucket/task3`

2. Erstellen Sie drei DataSync Aufgaben mit dem Namen task1, task2, und task3 die an das entsprechende Präfix in MyBucket übertragen werden.

Wählen Sie einen Aufgabenmodus für Ihre Datenübertragung

Ihre AWS DataSync Aufgabe kann in einem der folgenden Modi ausgeführt werden:

- **Erweiterter Modus** — Überträgt eine praktisch unbegrenzte Anzahl von Dateien oder Objekten mit höherer Leistung als der Standardmodus. Aufgaben im erweiterten Modus optimieren den Datenübertragungsprozess, indem sie Daten parallel auflisten, vorbereiten, übertragen und verifizieren. Der erweiterte Modus ist derzeit für Übertragungen zwischen Amazon S3-Standorten, Übertragungen zwischen Amazon S3 Azure Blob und Amazon S3 ohne Agenten, Übertragungen zwischen anderen Clouds und Amazon S3 ohne Agenten sowie Übertragungen zwischen NFS- oder SMB-Dateiservern und Amazon S3 mit einem Agenten im erweiterten Modus verfügbar.
- **Basismodus** — Übertragung von Dateien oder Objekten zwischen AWS Speicher und allen anderen unterstützten DataSync Speicherorten. Für Aufgaben im Basismodus gelten [Kontingente](#) für die Anzahl der Dateien, Objekte und Verzeichnisse in einem Datensatz. Im Basismodus werden Daten sequenziell vorbereitet, übertragen und überprüft, sodass er für die meisten Workloads langsamer ist als der erweiterte Modus.

Die Unterschiede im Aufgabenmodus verstehen

Anhand der folgenden Informationen können Sie ermitteln, welcher Taskmodus verwendet werden soll.

Funktion	Verbessertes Modusverhalten	Grundlegendes Verhalten im Modus
Leistung	DataSync listet, bereitet, überträgt und verifiziert Ihre Daten parallel. Bietet für die meisten Workloads (z. B. die Übertragung großer Objekte) eine höhere Leistung als der Basismodus	DataSync bereitet Ihre Daten nacheinander vor, überträgt und verifiziert sie. Die Leistung ist bei den meisten Workloads langsamer als im erweiterten Modus

Funktion	Verbessertes Modusverhalten	Grundlegendes Verhalten im Modus
Anzahl der Elemente in einem Datensatz, mit denen pro Aufgabenausführung gearbeitet werden DataSync kann	Praktisch unbegrenzte Anzahl von Objekten	Es gelten Kontingente
Zähler und Metriken für die Datenübertragung	Mehr Zähler und Messwerte als im Basismodus, z. B. die Anzahl der Objekte, die an Ihrem Quellspeicherort DataSync gefunden werden, die Anzahl der Objekte, die bei jeder Aufgabenausführung vorbereitet wurden, und Ordnerzähler, die den Datei- und Objektzählern ähneln	Weniger Zähler und Metriken als im erweiterten Modus
Protokollierung	Strukturierte Protokolle (JSON-Format)	Unstrukturierte Protokolle
Unterstützte Standorte	Derzeit für Übertragungen zwischen Amazon S3-Standorten, Übertragungen zwischen Azure Blob und Amazon S3 ohne Agenten, Übertragungen zwischen anderen Clouds und Amazon S3 ohne Agenten und Übertragungen zwischen NFS- oder SMB-Dateiservern und Amazon S3 mit einem Agenten im erweiterten Modus.	Für Übertragungen zwischen allen Standorten, die unterstützt werden DataSync

Funktion	Verbessertes Modusverhalten	Grundlegendes Verhalten im Modus
Optionen zur Datenüberprüfung	DataSync verifiziert nur übertragene Daten	DataSync verifiziert standardmäßig alle Daten
Bandbreitenbeschränkungen	Nicht zutreffend	Unterstützt
Cost (Kosten)	Weitere Informationen finden Sie auf der DataSync Preisseite	Weitere Informationen finden Sie auf der DataSync Preisseite
Fehlerbehandlung bei nicht unterstützten Objekt-Tags	Bei Cloud-Speicherübertragungen zu oder von Orten, die Objekt-Tagging nicht unterstützen, schlägt die Aufgabenausführung sofort fehl, wenn die <code>ObjectTags</code> Option nicht spezifiziert oder auf <code>gesetzt</code> ist. <code>PRESERVE</code>	Bei Cloud-Speicherübertragungen zu oder von Orten, die Objekt-Tagging nicht unterstützen, wird die Aufgabenausführung normal ausgeführt, aber es werden Fehler pro Objekt für markierte Objekte gemeldet, wenn die <code>ObjectTags</code> Option nicht spezifiziert oder auf <code>gesetzt</code> ist. <code>PRESERVE</code>

Einen Aufgabenmodus wählen

Sie können den erweiterten Modus nur für Übertragungen zwischen Amazon S3-Standorten, Übertragungen zwischen Azure Blob und Amazon S3 ohne Agenten, Übertragungen zwischen anderen Clouds und Amazon S3 ohne Agenten und Übertragungen zwischen NFS- oder SMB-Dateiservern und Amazon S3 mit einem Agenten im erweiterten Modus wählen. Andernfalls müssen Sie den Basismodus verwenden. Beispielsweise erfordert eine Übertragung von einem lokalen [HDFS-Standort](#) zu einem S3-Standort den Basismodus.

Ihre Aufgabenoptionen und Leistung können je nach ausgewähltem Aufgabenmodus variieren. Sobald Sie Ihre Aufgabe erstellt haben, können Sie den Aufgabenmodus nicht mehr ändern.

Erforderliche Berechtigungen

Um eine Aufgabe im erweiterten Modus zu erstellen, muss die IAM-Rolle, die Sie DataSync mit verwenden, über die `iam:CreateServiceLinkedRole` entsprechende Berechtigung verfügen.

Für Ihre DataSync Benutzerberechtigungen sollten Sie die Verwendung von [AWSDataSyncFullAccess](#). Dies ist eine AWS verwaltete Richtlinie, die einem Benutzer vollen DataSync und minimalen Zugriff auf seine Abhängigkeiten gewährt.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Wählen Sie für den Aufgabenmodus eine der folgenden Optionen:
 - Verbessert
 - Basic

Weitere Informationen finden Sie unter [Die Unterschiede im Aufgabenmodus verstehen](#).

5. Wählen Sie auf der Seite „Einstellungen konfigurieren“ andere Aufgabenoptionen aus oder verwenden Sie die Standardeinstellungen.

Einige der folgenden Optionen könnten Sie interessieren:

- Geben Sie mithilfe eines [Manifests](#) oder von [Filtern](#) an, welche Daten übertragen werden sollen.
- Konfigurieren Sie, wie [Dateimetadaten behandelt](#) werden sollen, und [überprüfen Sie die Datenintegrität](#).
- Überwachen Sie Ihre Übertragung mit [Aufgabenberichten](#) oder [Amazon CloudWatch Logs](#).

Wählen Sie abschließend Weiter.

6. Überprüfen Sie Ihre Aufgabenkonfiguration und wählen Sie dann Aufgabe erstellen.

Verwenden Sie den AWS CLI

1. Stellen Sie in Ihren AWS CLI Einstellungen sicher, dass Sie eines der Geräte verwenden, von AWS-Regionen denen Sie Daten übertragen möchten.
2. Kopieren Sie den folgenden create-task Befehl:

```
aws datasync create-task \  
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --task-mode "ENHANCED-or-BASIC"
```

3. Geben Sie für --source-location-arn den Amazon-Ressourcennamen (ARN) Ihres Quellstandorts an.
4. Geben Sie für --destination-location-arn den ARN Ihres Zielorts an.

Wenn du zwischen AWS-Regionen unseren Konten überweist, vergewissere dich, dass der ARN die andere Region oder Konto-ID enthält.

5. Geben Sie für --task-mode ENHANCED oder anBASIC.

Weitere Informationen finden Sie unter [Die Unterschiede im Aufgabenmodus verstehen](#).

6. Geben Sie nach Bedarf weitere Aufgabenoptionen an. Einige der folgenden Optionen könnten Sie interessieren:
 - Geben Sie mithilfe eines [Manifests](#) oder von [Filtern](#) an, welche Daten übertragen werden sollen.
 - Konfigurieren Sie, wie [Dateimetadaten behandelt](#) werden sollen, und [überprüfen Sie die Datenintegrität](#).
 - Überwachen Sie Ihre Übertragung mit [Aufgabenberichten](#) oder [Amazon CloudWatch Logs](#).

Weitere Optionen finden Sie unter Aufgabe [erstellen](#). Hier ist ein create-task Beispielfehl, der den erweiterten Modus und mehrere andere Optionen angibt:

```
aws datasync create-task \  

```

```
--source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
--destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
--name "task-name" \
--task-mode "ENHANCED" \
--options
TransferMode=CHANGED,VerifyMode=ONLY_FILES_TRANSFERRED,ObjectTags=PRESERVE,LogLevel=TRANSF
```

7. Führen Sie den Befehl `create-task` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN der Aufgabe anzeigt, die Sie erstellt haben. Beispiel:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Verwenden der DataSync API

Sie können den DataSync Aufgabenmodus angeben, indem Sie den `TaskMode` Parameter im [CreateTask](#) Vorgang konfigurieren.

Wählen Sie aus, welche AWS DataSync Übertragungen

AWS DataSync lässt Sie wählen, was übertragen werden soll und wie Ihre Daten behandelt werden sollen. Zu den Optionen gehören:

- Übertragung einer genauen Liste von Dateien oder Objekten mithilfe eines Manifests.
- Mithilfe eines Filters können Sie bestimmte Datentypen in Ihre Übertragung einbeziehen oder ausschließen.
- Bei wiederkehrenden Übertragungen werden nur die Daten verschoben, die sich seit der letzten Übertragung geändert haben
- Überschreiben von Daten am Zielspeicherort, sodass sie mit den Daten am Quellspeicherort übereinstimmen.
- Wählen Sie aus, welche Datei- oder Objektmetadaten zwischen Ihren Speicherorten beibehalten werden sollen.

Themen

- [Übertragung bestimmter Dateien oder Objekte mithilfe eines Manifests](#)
- [Übertragung bestimmter Dateien, Objekte und Ordner mithilfe von Filtern](#)
- [Verstehen, wie DataSync mit Datei- und Objektmetadaten umgegangen wird](#)
- [Links und Verzeichnisse, die kopiert wurden von AWS DataSync](#)
- [Konfiguration des Umgangs mit Dateien, Objekten und Metadaten](#)

Übertragung bestimmter Dateien oder Objekte mithilfe eines Manifests

Ein Manifest ist eine Liste von Dateien oder Objekten, die Sie übertragen AWS DataSync möchten. Anstatt beispielsweise alles in einem S3-Bucket mit potenziell Millionen von Objekten übertragen zu müssen, werden nur die Objekte DataSync übertragen, die Sie in Ihrem Manifest auflisten.

Manifeste ähneln [Filtern](#), ermöglichen es Ihnen aber, anstelle von Daten, die einem Filtermuster entsprechen, genau zu identifizieren, welche Dateien oder Objekte übertragen werden sollen.

Note

Die maximal zulässige Größe für eine Manifestdatei mit Aufgaben im erweiterten Modus beträgt 20 GB.

Erstellen Sie Ihr Manifest

Ein Manifest ist eine Datei im CSV-Format (Comma-Separated Values), in der die Dateien oder Objekte an Ihrem Quellspeicherort aufgeführt sind, die Sie übertragen möchten. DataSync Wenn es sich bei Ihrer Quelle um einen S3-Bucket handelt, können Sie auch angeben, welche Version eines Objekts übertragen werden soll.

Themen

- [Richtlinien](#)
- [Beispielmanifeste](#)

Richtlinien

Verwenden Sie diese Richtlinien, um ein Manifest zu erstellen, mit dem Sie arbeiten können DataSync.

Do

- Geben Sie den vollständigen Pfad jeder Datei oder jedes Objekts an, das Sie übertragen möchten.

Sie können nicht nur ein Verzeichnis oder einen Ordner angeben, um den gesamten Inhalt zu übertragen. In diesen Situationen sollten Sie einen [Include-Filter](#) anstelle eines Manifests verwenden.

- Stellen Sie sicher, dass jeder Datei- oder Objektpfad relativ zu dem Bereitstellungspfad, Ordner, Verzeichnis oder Präfix ist, das Sie bei der Konfiguration Ihres DataSync Quellverzeichnisses angegeben haben.

Nehmen wir zum Beispiel an, Sie [konfigurieren einen S3-Standort](#) mit einem Präfix namens `photos`. Dieses Präfix enthält ein Objekt `my-picture.png`, das Sie übertragen möchten. Im Manifest müssen Sie dann nur das Objekt (`my-picture.png`) anstelle des Präfixes und des Objekts (`photos/my-picture.png`) angeben.

- Um die Amazon S3 S3-Objektversion anzugeben IDs, trennen Sie den Pfad und die Versions-ID des Objekts durch ein Komma.

Das folgende Beispiel zeigt einen Manifesteintrag mit zwei Feldern. Das erste Feld enthält ein Objekt mit dem Namen `picture1.png`. Das zweite Feld ist durch ein Komma getrennt und enthält die Versions-ID: `111111`

```
picture1.png,111111
```

- Verwenden Sie Anführungszeichen in den folgenden Situationen:
 - Wenn ein Pfad Sonderzeichen (Kommas, Anführungszeichen und Zeilenenden) enthält:

```
"filename,with,commas.txt"
```

- Wenn sich ein Pfad über mehrere Zeilen erstreckt:

```
"this  
is  
a  
filename.txt"
```

- Wenn ein Pfad Anführungszeichen enthält:

```
filename""with""quotes.txt
```

Dies stellt einen Pfad mit dem Namen `darfilename"with"quotes.txt`.

Diese Regeln für Anführungszeichen gelten auch für Versions-ID-Felder. Wenn ein Manifestfeld ein Anführungszeichen enthält, müssen Sie es im Allgemeinen mit einem anderen Anführungszeichen versehen.

- Trennen Sie jeden Datei- oder Objekteintrag durch eine neue Zeile.

Sie können Zeilen trennen, indem Sie Zeilenumbrüche im Linux-Stil (Zeilenvorschub oder Zeilenumbruch) oder Windows (Zeilenumbruch gefolgt von einem Zeilenvorschub) verwenden.

- Speichern Sie Ihr Manifest (zum Beispiel `my-manifest.csv` oder `my-manifest.txt`).
- Laden Sie das Manifest in einen S3-Bucket hoch, der [darauf zugreifen DataSync kann](#).

Dieser Bucket muss sich nicht in demselben AWS-Region PR-Konto befinden, das Sie verwenden DataSync.

Don't

- Geben Sie nur ein Verzeichnis oder einen Ordner an, um den gesamten Inhalt zu übertragen.

Ein Manifest kann nur vollständige Pfade zu den Dateien oder Objekten enthalten, die Sie übertragen möchten. Wenn Sie Ihren Quellpfad so konfigurieren, dass er einen bestimmten Bereitstellungspfad, Ordner, Verzeichnis oder Präfix verwendet, müssen Sie dies nicht in Ihr Manifest aufnehmen.

- Geben Sie einen Datei- oder Objektpfad an, der mehr als 4.096 Zeichen enthält.
- Geben Sie einen Dateipfad, Objektpfad oder eine Amazon S3 S3-Objektversions-ID an, die 1.024 Byte überschreitet.
- Geben Sie doppelte Datei- oder Objektpfade an.
- Geben Sie eine Objekt-Versions-ID an, wenn es sich bei Ihrem Quellspeicherort nicht um einen S3-Bucket handelt.
- Fügen Sie mehr als zwei Felder in einen Manifesteintrag ein.

Ein Eintrag kann nur einen Datei- oder Objektpfad und (falls zutreffend) eine Amazon S3 S3-Objektversions-ID enthalten.

- Schließt Zeichen ein, die nicht der UTF-8-Kodierung entsprechen.

- Fügen Sie unbeabsichtigte Leerzeichen in Ihre Eingabefelder außerhalb von Anführungszeichen ein.

Beispielmanifeste

Verwenden Sie diese Beispiele, um ein Manifest zu erstellen, das mit funktioniert DataSync.

Manifest mit vollständigen Datei- oder Objektpfaden

Das folgende Beispiel zeigt ein Manifest mit vollständigen Datei- oder Objektpfaden für die Übertragung.

```
photos/picture1.png  
photos/picture2.png  
photos/picture3.png
```

Manifest nur mit Objektschlüsseln

Das folgende Beispiel zeigt ein Manifest mit Objekten, die von einem Amazon S3 S3-Quellspeicherort übertragen werden sollen. Da der [Standort mit dem Präfix konfiguriert ist](#) photos, werden nur die Objektschlüssel angegeben.

```
picture1.png  
picture2.png  
picture3.png
```

Manifest mit Objektpfaden und Version IDs

Die ersten beiden Einträge im folgenden Manifestbeispiel enthalten spezifische Amazon S3 S3-Objektversionen, die übertragen werden sollen.

```
photos/picture1.png,111111  
photos/picture2.png,121212  
photos/picture3.png
```

Manifest mit UTF-8-Zeichen

Das folgende Beispiel zeigt ein Manifest mit Dateien, die UTF-8-Zeichen enthalten.

```
documents/résumé1.pdf  
documents/résumé2.pdf
```

documents/résumé3.pdf

Bereitstellung des DataSync Zugriffs auf Ihr Manifest

Sie benötigen eine AWS Identity and Access Management (IAM-) Rolle, die DataSync Zugriff auf Ihr Manifest in seinem S3-Bucket gewährt. Diese Rolle muss die folgenden Berechtigungen beinhalten:

- `s3:GetObject`
- `s3:GetObjectVersion`

Sie können diese Rolle automatisch in der DataSync Konsole generieren oder sie selbst erstellen.

Note

Wenn sich Ihr Manifest in einem anderen befindet AWS-Konto, müssen Sie diese Rolle manuell erstellen.

Automatisches Erstellen der IAM-Rolle

Wenn Sie eine Übertragungsaufgabe in der Konsole erstellen oder starten, DataSync kann für Sie eine IAM-Rolle mit den `s3:GetObjectVersion` Berechtigungen `s3:GetObject` und Berechtigungen, die Sie für den Zugriff auf Ihr Manifest benötigen, erstellen.

Erforderliche Berechtigungen, um die Rolle automatisch zu erstellen

Um die Rolle automatisch zu erstellen, stellen Sie sicher, dass die Rolle, die Sie für den Zugriff auf die DataSync Konsole verwenden, über die folgenden Berechtigungen verfügt:

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:AttachRolePolicy`

Die IAM-Rolle erstellen (gleiches Konto)

Sie können die IAM-Rolle, die auf Ihr Manifest zugreifen DataSync muss, manuell erstellen. In den folgenden Anweisungen wird davon ausgegangen, dass Sie sich dort befinden, AWS-Konto wo Sie es verwenden, DataSync und dass sich der S3-Bucket Ihres Manifests befindet.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen und dann Rolle erstellen aus.
3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option AWS-Service.
4. Wählen Sie DataSync in der Dropdownliste für Anwendungsfall die Option aus und wählen Sie aus DataSync. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus. Geben Sie Ihrer Rolle einen Namen und wählen Sie Rolle erstellen.
6. Suchen Sie auf der Seite Rollen nach der Rolle, die Sie gerade erstellt haben, und wählen Sie ihren Namen aus.
7. Wählen Sie auf der Detailseite der Rolle den Tab Berechtigungen aus. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
8. Wählen Sie die Registerkarte JSON und fügen Sie die folgende Beispielrichtlinie in den Richtlinieneditor ein:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DataSyncAccessManifest",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/my-manifest.csv"
  }]
}
```

9. Ersetzen Sie in der Beispielrichtlinie, die Sie gerade eingefügt haben, die folgenden Werte durch Ihre eigenen:
 - a. *amzn-s3-demo-bucket* Ersetzen Sie es durch den Namen des S3-Buckets, der Ihr Manifest hostet.
 - b. *my-manifest.csv* Ersetzen Sie es durch den Dateinamen Ihres Manifests.

10. Wählen Sie Weiter aus. Geben Sie Ihrer Richtlinie einen Namen und wählen Sie Richtlinie erstellen.
11. (Empfohlen) Gehen Sie wie folgt vor, um das [dienstübergreifende Problem mit verwirrten Stellvertretern](#) zu vermeiden:
 - a. Wählen Sie auf der Detailseite der Rolle die Registerkarte Vertrauensbeziehungen aus. Wählen Sie Vertrauensrichtlinie bearbeiten aus.
 - b. Aktualisieren Sie die Vertrauensrichtlinie anhand des folgenden Beispiels, das die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel enthält:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "555555555555"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:datasync:us-east-1:555555555555:*"
        }
      }
    }
  ]
}
```

- Ersetzen Sie jede Instanz *account-id* durch die AWS-Konto ID, die Sie verwenden DataSync.
 - Ersetze es *region* durch das AWS-Region , wo du es verwendest DataSync.
- c. Wählen Sie Richtlinie aktualisieren.

Sie haben eine IAM-Rolle erstellt, die den Zugriff DataSync auf Ihr Manifest ermöglicht. Geben Sie diese Rolle an, wenn Sie Ihre Aufgabe [erstellen](#) oder [starten](#).

Die IAM-Rolle erstellen (anderes Konto)

Wenn sich Ihr Manifest in einem S3-Bucket befindet, der zu einem anderen gehört AWS-Konto, müssen Sie die IAM-Rolle, die für den Zugriff auf das Manifest DataSync verwendet wird, manuell erstellen. Anschließend müssen Sie dort, AWS-Konto wo sich Ihr Manifest befindet, die Rolle in die S3-Bucket-Richtlinie aufnehmen.

Erstellen der -Rolle

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen und dann Rolle erstellen aus.
3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option AWS-Service.
4. Wählen Sie DataSync in der Dropdownliste für Anwendungsfall die Option aus und wählen Sie aus DataSync. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus. Geben Sie Ihrer Rolle einen Namen und wählen Sie Rolle erstellen.
6. Suchen Sie auf der Seite Rollen nach der Rolle, die Sie gerade erstellt haben, und wählen Sie ihren Namen aus.
7. Wählen Sie auf der Detailseite der Rolle den Tab Berechtigungen aus. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
8. Wählen Sie die Registerkarte JSON und fügen Sie die folgende Beispielrichtlinie in den Richtlinieneditor ein:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DataSyncAccessManifest",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
```

```

    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/my-manifest.csv"
  }]
}

```

9. Ersetzen Sie in der Beispielrichtlinie, die Sie gerade eingefügt haben, die folgenden Werte durch Ihre eigenen:
 - a. *amzn-s3-demo-bucket* Ersetzen Sie es durch den Namen des S3-Buckets, der Ihr Manifest hostet.
 - b. *my-manifest.csv* Ersetzen Sie es durch den Dateinamen Ihres Manifests.
10. Wählen Sie Weiter aus. Geben Sie Ihrer Richtlinie einen Namen und wählen Sie Richtlinie erstellen.
11. (Empfohlen) Gehen Sie wie folgt vor, um das [dienstübergreifende Problem mit verwirrten Stellvertretern](#) zu vermeiden:
 - a. Wählen Sie auf der Detailseite der Rolle die Registerkarte Vertrauensbeziehungen aus. Wählen Sie Vertrauensrichtlinie bearbeiten aus.
 - b. Aktualisieren Sie die Vertrauensrichtlinie anhand des folgenden Beispiels, das die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel enthält:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "000000000000"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:datasync:us-east-1:000000000000:*"
        }
      }
    }
  ]
}

```

```

    }
  }
]
}

```

- Ersetzen Sie jede Instanz von *account-id* durch die AWS-Konto ID, die Sie verwenden DataSync.
 - Ersetze es *region* durch die AWS-Region Stelle, die du verwendest DataSync.
- c. Wählen Sie Richtlinie aktualisieren.

Sie haben die IAM-Rolle erstellt, die Sie in Ihre S3-Bucket-Richtlinie aufnehmen können.

Aktualisierung Ihrer S3-Bucket-Richtlinie mit der Rolle

Nachdem Sie die IAM-Rolle erstellt haben, müssen Sie sie der S3-Bucket-Richtlinie in der anderen Rolle hinzufügen, in der AWS-Konto sich Ihr Manifest befindet.

1. Wechseln Sie im AWS-Managementkonsole zu dem Konto mit dem S3-Bucket Ihres Manifests.
2. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
3. Wählen Sie auf der Detailseite des Buckets den Tab Permissions aus.
4. Wählen Sie unter Bucket-Richtlinie die Option Bearbeiten aus und gehen Sie wie folgt vor, um Ihre S3-Bucket-Richtlinie zu ändern:
 - a. Aktualisieren Sie den Inhalt des Editors, sodass er die folgenden Richtlinienerklärungen enthält:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncAccessManifestBucket",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
    }
  ],
}

```

```
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
  }
]
}
```

- b. **account-id** Ersetzen Sie es durch die AWS-Konto ID für das Konto, das Sie DataSync mit verwenden.
 - c. **datasync-role** Ersetzen Sie es durch die IAM-Rolle, die Sie gerade erstellt haben und die DataSync den Zugriff auf Ihr Manifest ermöglicht.
 - d. **amzn-s3-demo-bucket** Ersetzen Sie es im anderen AWS-Konto durch den Namen des S3-Buckets, der Ihr Manifest hostet.
5. Wählen Sie **Änderungen speichern** aus.

Sie haben eine IAM-Rolle erstellt, die DataSync den Zugriff auf Ihr Manifest in dem anderen Konto ermöglicht. Geben Sie diese Rolle an, wenn Sie Ihre Aufgabe [erstellen](#) oder [starten](#).

Geben Sie Ihr Manifest an, wenn Sie eine Aufgabe erstellen

Sie können das Manifest angeben, das Sie beim Erstellen einer Aufgabe verwenden möchten DataSync .

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich **Aufgaben** und dann **Aufgabe erstellen** aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Wählen Sie unter **Zu scannende Inhalte** die Option **Bestimmte Dateien, Objekte und Ordner** und anschließend **Manifest verwenden** aus.
5. Wählen Sie für **S3-URI** Ihr Manifest aus, das auf einem S3-Bucket gehostet wird.

Alternativ können Sie den URI eingeben (z. B. `s3://bucket/prefix/my-manifest.csv`).

6. Wählen Sie unter **Objektversion** die Version des Manifests aus, die Sie verwenden DataSync möchten.

DataSync Verwendet standardmäßig die neueste Version des Objekts.

7. Führen Sie für die Zugriffsrolle Manifest einen der folgenden Schritte aus:

- Wählen Sie Autogenerate für DataSync , um automatisch eine IAM-Rolle mit den erforderlichen Berechtigungen für den Zugriff auf Ihr Manifest in ihrem S3-Bucket zu erstellen.
- Wählen Sie eine bestehende IAM-Rolle aus, die auf Ihr Manifest zugreifen kann.

Weitere Informationen finden Sie unter [Bereitstellung des DataSync Zugriffs auf Ihr Manifest](#).

8. Konfigurieren Sie alle anderen Aufgabeneinstellungen, die Sie benötigen, und wählen Sie dann Weiter.
9. Wählen Sie Create task aus.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden create-task Befehl:

```
aws datasync create-task \  
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/  
loc-12345678abcdefgh \\  
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/loc-  
abcdefgh12345678 \  
  --manifest-config {  
    "Source": {  
      "S3": {  
        "ManifestObjectPath": "s3-object-key-of-manifest",  
        "BucketAccessRoleArn": "bucket-iam-role",  
        "S3BucketArn": "amzn-s3-demo-bucket-arn",  
        "ManifestObjectVersionId": "manifest-version-to-use"  
      }  
    }  
  }
```

2. Geben Sie für den --source-location-arn Parameter den Amazon-Ressourcennamen (ARN) des Standorts an, von dem Sie Daten übertragen.
3. Geben Sie für den --destination-location-arn Parameter den ARN des Standorts an, an den Sie Daten übertragen.
4. Gehen Sie für den --manifest-config Parameter wie folgt vor:
- ManifestObjectPath— Geben Sie den S3-Objektschlüssel Ihres Manifests an.

- `BucketAccessRoleArn`— Geben Sie die IAM-Rolle an, die den DataSync Zugriff auf Ihr Manifest in ihrem S3-Bucket ermöglicht.

Weitere Informationen finden Sie unter [Bereitstellung des DataSync Zugriffs auf Ihr Manifest](#).

- `S3BucketArn`— Geben Sie den ARN des S3-Buckets an, der Ihr Manifest hostet.
- `ManifestObjectVersionId`— Geben Sie die Version des Manifests an, die Sie verwenden DataSync möchten.

DataSync Verwendet standardmäßig die neueste Version des Objekts.

5. Führen Sie den `create-task` Befehl aus, um Ihre Aufgabe zu erstellen.

Wenn Sie bereit sind, können Sie [Ihre Übertragungsaufgabe starten](#).

Geben Sie Ihr Manifest an, wenn Sie eine Aufgabe starten

Sie können das Manifest angeben, das Sie beim Ausführen einer Aufgabe verwenden möchten DataSync .

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich Aufgaben und dann die Aufgabe aus, die Sie starten möchten.
3. Wählen Sie auf der Seite mit der Aufgabenübersicht die Option Start und dann Mit überschreibenden Optionen beginnen aus.
4. Wählen Sie unter Zu scannende Inhalte die Option Bestimmte Dateien, Objekte und Ordner und anschließend Manifest verwenden aus.
5. Wählen Sie für S3-URI Ihr Manifest aus, das auf einem S3-Bucket gehostet wird.

Alternativ können Sie den URI eingeben (z. B. `s3://bucket/prefix/my-manifest.csv`).

6. Wählen Sie unter Objektversion die Version des Manifests aus, die Sie verwenden DataSync möchten.

DataSync Verwendet standardmäßig die neueste Version des Objekts.

7. Führen Sie für die Zugriffsrolle Manifest einen der folgenden Schritte aus:

- Wählen Sie Automatisch generieren für DataSync, um automatisch eine IAM-Rolle für den Zugriff auf Ihr Manifest in Ihrem S3-Bucket zu erstellen.
- Wählen Sie eine bestehende IAM-Rolle aus, die auf Ihr Manifest zugreifen kann.

Weitere Informationen finden Sie unter [Bereitstellung des DataSync Zugriffs auf Ihr Manifest](#).

8. Wählen Sie Start, um mit der Übertragung zu beginnen.

Mit dem AWS CLI

1. Kopieren Sie den folgenden start-task-execution Befehl:

```
aws datasync start-task-execution \  
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh \  
  --manifest-config {  
    "Source": {  
      "S3": {  
        "ManifestObjectPath": "s3-object-key-of-manifest",  
        "BucketAccessRoleArn": "bucket-iam-role",  
        "S3BucketArn": "amzn-s3-demo-bucket-arn",  
        "ManifestObjectVersionId": "manifest-version-to-use"  
      }  
    }  
  }
```

2. Geben Sie für den --task-arn Parameter den Amazon-Ressourcennamen (ARN) der Aufgabe an, die Sie starten.
3. Gehen Sie für den --manifest-config Parameter wie folgt vor:

- ManifestObjectPath— Geben Sie den S3-Objektschlüssel Ihres Manifests an.
- BucketAccessRoleArn— Geben Sie die IAM-Rolle an, die den DataSync Zugriff auf Ihr Manifest in Ihrem S3-Bucket ermöglicht.

Weitere Informationen finden Sie unter [Bereitstellung des DataSync Zugriffs auf Ihr Manifest](#).

- S3BucketArn— Geben Sie den ARN des S3-Buckets an, der Ihr Manifest hostet.
- ManifestObjectVersionId— Geben Sie die Version des Manifests an, die Sie verwenden möchten.

DataSync Verwendet standardmäßig die neueste Version des Objekts.

4. Führen Sie den `start-task-execution` Befehl aus, um mit der Übertragung zu beginnen.

Einschränkungen

- Sie können ein Manifest nicht zusammen mit [Filtern](#) verwenden.
- Sie können nicht nur ein Verzeichnis oder einen Ordner angeben, um dessen gesamten Inhalt zu übertragen. In diesen Situationen sollten Sie einen [Include-Filter](#) anstelle eines Manifests verwenden.
- Sie können die Aufgabenoption Gelöschte Dateien behalten (`PreserveDeletedFiles` in der [API](#)) nicht verwenden, um [Dateien oder Objekte im Ziel zu verwalten, die sich nicht in der Quelle befinden](#). DataSync überträgt nur das, was in Ihrem Manifest aufgeführt ist, und löscht nichts im Ziel.

Fehlerbehebung

Fehler im Zusammenhang mit **HeadObject** oder **GetObjectTagging**

Wenn Sie Objekte mit einer bestimmten Version IDs aus einem S3-Bucket übertragen, wird möglicherweise ein Fehler im Zusammenhang mit `HeadObject` oder `getObjectTagging` angezeigt. Hier ist zum Beispiel ein Fehler im Zusammenhang mit `GetObjectTagging`:

```
[WARN] Failed to read metadata for file /picture1.png (versionId: 111111): S3 Get
Object Tagging Failed
[ERROR] S3 Exception: op=GetObjectTagging photos/picture1.png, code=403, type=15,
exception=AccessDenied,
msg=Access Denied req-hdrs: content-type=application/xml, x-amz-api-version=2006-03-01
rsp-hdrs: content-type=application/xml,
date=Wed, 07 Feb 2024 20:16:14 GMT, server=AmazonS3, transfer-encoding=chunked,
x-amz-id-2=I0WQ4fDEXAMPLEQM+ey7N9WgVhSnQ6JEXAMPLEZb7hSQDASK+Jd1vEXAMPLEa3Km, x-amz-
request-id=79104EXAMPLEB723
```

Wenn Sie einen dieser Fehler sehen, überprüfen Sie, ob die IAM-Rolle, die für den Zugriff auf Ihren S3-Quellspeicherort DataSync verwendet wird, über die folgenden Berechtigungen verfügt:

- `s3:GetObjectVersion`

- `s3:GetObjectVersionTagging`

Informationen dazu, wie Sie Ihre Rolle mit diesen Berechtigungen aktualisieren müssen, finden Sie unter [Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort](#).

Fehler: **ManifestFileDoesNotExist**

Dieser Fehler weist darauf hin, dass eine Datei im Manifest nicht an der Quelle gefunden wurde. Lesen Sie die [Richtlinien](#) für die Erstellung eines Manifests.

Nächste Schritte

Falls Sie es noch nicht getan haben, [beginnen Sie mit Ihrer Aufgabe](#). [Überwachen Sie andernfalls die Aktivität Ihrer Aufgabe](#).

Übertragung bestimmter Dateien, Objekte und Ordner mithilfe von Filtern

AWS DataSync ermöglicht das Anwenden von Filtern, um Daten von Ihrem Quellspeicherort in eine Übertragung ein- oder auszuschließen. Wenn Sie beispielsweise keine temporären Dateien übertragen möchten, die mit `.tmp` enden, können Sie einen Ausschlussfilter erstellen, sodass diese Dateien nicht an Ihren Zielort gelangen.

Sie können in derselben Übertragungsaufgabe eine Kombination aus Ausschluss- und Einschließenfiltern verwenden. Wenn Sie die Filter einer Aufgabe ändern, werden diese Änderungen übernommen, wenn Sie die Aufgabe das nächste Mal ausführen.

Begriffe, Definitionen und Syntax filtern

Machen Sie sich mit den Konzepten rund um das DataSync Filtern vertraut:

Filter

Die gesamte Zeichenfolge, aus der ein bestimmter Filter besteht (z. B. `*.tmp | *.temp oder/ folderA|/folderB`).

Filter bestehen aus Mustern, die durch einen senkrechten Strich (`|`) voneinander getrennt werden. Sie benötigen kein Trennzeichen, wenn Sie Muster in der DataSync Konsole hinzufügen, da Sie jedes Muster separat hinzufügen.

Note

Bei Filtern wird zwischen Groß- und Kleinschreibung unterschieden. Beispielsweise stimmt der Filter `/folderA` nicht überein mit `FolderA`.

Muster

Ein Muster innerhalb eines Filters. `*.tmp` ist beispielsweise ein Muster, das Teil des `*.tmp | *.temp` Filters ist. Wenn Ihr Filter mehrere Muster hat, grenzen Sie jedes Muster mit einem senkrechten Strich (`|`) ab.

Ordner

- Alle Filter beziehen sich auf den Quellverzeichnispfad. Nehmen wir beispielsweise an, dass Sie bei der Erstellung Ihres Quellspeicherorts und Ihrer Aufgabe den Quellpfad `/my_source/` als Quellpfad angeben und den Include-Filter `/transfer_this/` angeben. In diesem Fall werden nur das Verzeichnis `/my_source/transfer_this/` und sein Inhalt DataSync übertragen.
- Um einen Ordner direkt unter dem Quellverzeichnis anzugeben, fügen Sie vor dem Ordernamen einen Schrägstrich (`/`) ein. Im vorangehenden Beispiel wird für das Muster `/transfer_this` anstelle von `transfer_this` verwendet.
- DataSync interpretiert die folgenden Muster auf dieselbe Weise und entspricht sowohl dem Ordner als auch seinem Inhalt.

`/dir`

`/dir/`

- Wenn Sie Daten von oder in einen Amazon S3 S3-Bucket übertragen, DataSync behandelt das `/` Zeichen im Objektschlüssel als das Äquivalent eines Ordners in einem Dateisystem.

Sonderzeichen

Nachfolgend finden Sie Sonderzeichen für die Verwendung mit Filtern.

Sonderzeichen	Beschreibung
<code>*</code> (Platzhalter)	Ein Zeichen entspricht 0 oder mehr Zeichen. Beispiel: <code>/movies_folder*</code> entspricht sowohl <code>/movies_folder</code> als auch <code>/movies_folder1</code> .

Sonderzeichen	Beschreibung
(Pipe-Trennzeichen)	Dieses Zeichen wird als Trennzeichen zwischen Mustern verwendet. So können mehrere Muster angegeben werden, von denen beliebige mit dem Filter übereinstimmen können. Beispiel: *.tmp *.temp stimmt mit Dateien mit der Endung tmp oder temp überein.  Note Dieses Trennzeichen wird nicht benötigt, wenn Sie Muster auf der Konsole hinzufügen, da Sie jedes Muster in einer separaten Zeile hinzufügen.
\ (umgekehrter Schrägstrich)	Ein Zeichen, das als Escape-Zeichen (*, ,\) in einem Datei- oder Objektnamen verwendet wird. Ein doppelter umgekehrter Schrägstrich (\\) ist erforderlich, wenn ein umgekehrter Schrägstrich Teil eines Dateinamens ist. Entsprechend stellt \\\\ zwei aufeinander folgende umgekehrte Schrägstriche in einem Dateinamen dar. Ein umgekehrter Schrägstrich gefolgt von einer Pipe (\) ist erforderlich, wenn eine Pipe Teil eines Dateinamens ist. Ein umgekehrter Schrägstrich (\), gefolgt von einem anderen Zeichen oder am Ende eines Musters, wird ignoriert.

Beispielfilter

Die folgenden Beispiele zeigen gängige Filter, die Sie zusammen verwenden können DataSync.

Note

Die Anzahl der Zeichen, die Sie in einem Filter verwenden können, ist begrenzt. Weitere Informationen finden Sie unter [DataSync Kontingente](#).

Ausschließen bestimmter Ordner aus dem Quellverzeichnis

In einigen Fällen möchten Sie möglicherweise Ordner an Ihrem Quellspeicherort ausschließen, um sie nicht an Ihren Zielspeicherort zu kopieren. Wenn Sie beispielsweise über temporäre work-in-progress Ordner verfügen, können Sie etwa den folgenden Filter verwenden:

```
* /.temp
```

Um Ordner mit ähnlichem Inhalt (wie `/reports2021` und `/reports2022`)) auszuschließen, können Sie einen Ausschlussfilter wie den folgenden verwenden:

```
/reports*
```

Um Ordner auf einer beliebigen Ebene in der Dateihierarchie auszuschließen, können Sie einen Ausschlussfilter wie den folgenden verwenden.

```
*/folder-to-exclude-1|*/folder-to-exclude-2
```

Um Ordner auf der obersten Ebene des Quellspeicherorts auszuschließen, können Sie einen Ausschlussfilter wie den folgenden verwenden.

```
/top-level-folder-to-exclude-1|/top-level-folder-to-exclude-2
```

Schließen Sie eine Teilmenge der Ordner an Ihrem Quellspeicherort ein

In einigen Fällen kann es sich bei Ihrem Quellspeicherort um einen großen Anteil handeln, und Sie müssen eine Teilmenge der Ordner unter das Stammverzeichnis übertragen. Um bestimmte Ordner einzuschließen, starten Sie eine Aufgabenausführung mit einem einschließenden Filter wie folgt.

```
/folder-to-transfer/*
```

Ausschließen bestimmter Dateitypen

Um bestimmte Dateitypen während der Übertragung auszuschließen, können Sie eine Aufgabenausführung mit einem ausschließenden Filter wie `*.temp` erstellen.

Übertragen Sie einzelne Dateien, die Sie angeben

Um eine Liste einzelner Dateien zu übertragen, starten Sie eine Aufgabenausführung mit einem Include-Filter wie dem folgenden: `"/folder/subfolder/file1.txt|/folder/subfolder/file2.txt |/folder/subfolder/file2.txt"`

Include-Filter erstellen

Einschlussfilter definieren die Dateien, Objekte und Ordner, die Sie übertragen DataSync möchten. Sie können Einschlussfilter konfigurieren, wenn Sie eine Aufgabe erstellen, bearbeiten oder starten.

DataSync scannt und überträgt nur Dateien und Ordner, die den Einschlussfiltern entsprechen. Um beispielsweise eine Teilmenge Ihrer Quellordner einzubeziehen, können Sie `/important_folder_1 | /important_folder_2` angeben.

Note

Einschließende Filter unterstützen das Platzhalterzeichen (*) nur als Zeichen ganz rechts in einem Muster. Zum Beispiel `/code*` wird `/documents* |` unterstützt, aber `*.txt` nicht.

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich Aufgaben und dann Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#)

4. Wählen Sie unter Zu scannende Inhalte die Option Bestimmte Dateien, Objekte und Ordner und anschließend Filter verwenden aus.
5. Geben Sie unter Eingeschlossen Ihren Filter ein (z. B. `/important_folders` um ein wichtiges Verzeichnis einzubeziehen) und wählen Sie dann Muster hinzufügen aus.
6. Fügen Sie nach Bedarf weitere Include-Filter hinzu.

Mit dem AWS CLI

Wenn Sie den Filter verwenden AWS CLI, müssen Sie einfache Anführungszeichen (') und ein | (senkrechter Strich) als Trennzeichen verwenden, wenn Sie mehr als einen Filter haben.

Im folgenden Beispiel werden zwei Include-Filter `/important_folder1` und `/important_folder2` bei der Ausführung des `create-task` Befehls angegeben.

```
aws datasync create-task
```

```
--source-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \  
--destination-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \  
\   
--includes FilterType=SIMPLE_PATTERN,Value='/important_folder1|/important_folder2'
```

Ausschlussfilter erstellen

Ausschlussfilter definieren die Dateien, Objekte und Ordner an Ihrem Quellspeicherort, die Sie nicht übertragen DataSync möchten. Sie können diese Filter konfigurieren, wenn Sie eine Aufgabe erstellen, bearbeiten oder starten.

Themen

- [Daten sind standardmäßig ausgeschlossen](#)

Daten sind standardmäßig ausgeschlossen

DataSync schließt einige Daten automatisch von der Übertragung aus:

- `.snapshot`— DataSync ignoriert alle Pfade, die mit `.snapshot` enden, was normalerweise für point-in-time Schnappschüsse der Dateien oder Verzeichnisse eines Speichersystems verwendet wird.
- `/.aws-datasync` und `/.awssync` — DataSync erstellt diese Ordner an Ihrem Standort, um Ihre Übertragung zu erleichtern.
- `/.zfs`— Möglicherweise sehen Sie diesen Ordner bei Amazon FSx für OpenZFS-Speicherorte.

Verwenden der Konsole DataSync

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich Aufgaben und dann Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#)

4. Geben Sie unter Ausschlüsse Ihren Filter ein (z. B. `*/temp` um temporäre Ordner auszuschließen) und wählen Sie dann Muster hinzufügen aus.
5. Fügen Sie nach Bedarf weitere Ausschlussfilter hinzu.
6. [Fügen Sie bei Bedarf Einschlussfilter](#) hinzu.

Mit dem AWS CLI

Wenn Sie den Filter verwenden AWS CLI, müssen Sie einfache Anführungszeichen (') und ein | (senkrechter Strich) als Trennzeichen verwenden, wenn Sie mehr als einen Filter haben.

Im folgenden Beispiel werden zwei Ausschlussfilter */temp und */tmp bei der Ausführung des create-task Befehls angegeben.

```
aws datasync create-task \  
  --source-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \  
  --destination-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \  
  \  
  --excludes FilterType=SIMPLE_PATTERN,Value='*/temp|*/tmp'
```

Verstehen, wie DataSync mit Datei- und Objektmetadaten umgegangen wird

AWS DataSync kann Ihre Datei- oder Objektmetadaten während einer Datenübertragung beibehalten. Wie Ihre Metadaten kopiert werden, hängt von Ihren Übertragungsorten ab und davon, ob diese Speicherorte ähnliche Arten von Metadaten verwenden.

Metadaten auf Systemebene

Kopiert im Allgemeinen DataSync keine Metadaten auf Systemebene. Wenn Sie beispielsweise Daten von einem SMB-Dateiserver übertragen, werden die Berechtigungen, die Sie auf Dateisystemebene konfiguriert haben, nicht auf das Zielspeichersystem kopiert.

Es gibt Ausnahmen. DataSync kopiert bei der Übertragung zwischen Amazon S3 und anderem Objektspeicher einige [systemdefinierte Objektmetadaten](#).

Metadaten, die bei Amazon S3 S3-Übertragungen kopiert wurden

In den folgenden Tabellen wird beschrieben, welche Metadaten kopiert DataSync werden können, wenn eine Übertragung einen Amazon S3 S3-Standort betrifft.

Themen

- [Zu Amazon S3](#)
- [Zwischen Amazon S3 und anderem Objektspeicher](#)
- [Zwischen Amazon S3 und HDFS](#)

Zu Amazon S3

Beim Kopieren von einem dieser Standorte	Zu diesem Ort	DataSync kann kopieren
• NFS • Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS)	• Amazon S3	Folgendes als Amazon S3 S3-Benutzermetadaten: • Zeitstempel für Datei- und Ordneränderungen • Zeitstempel für den Datei- und Ordnerzugriff (DataSync dies ist nur nach bestem Wissen möglich) • Benutzer-ID und Gruppen-ID • POSIX-Berechtigungen Die in Amazon S3 S3-Benutzermetadaten gespeicherten Dateimetadaten sind mit NFS-Shares auf File-Gateways kompatibel und verwenden . AWS Storage Gateway Ein File-Gateway ermöglicht den Zugriff mit niedriger Latenz von lokalen Netzwerken auf Daten, die von nach Amazon S3 kopiert wurden. DataSync Diese Metadaten sind auch mit for Lustre kompatibel FSx . Wenn Objekte, die diese Metadaten enthalten, zurück auf einen NFS-Server DataSync kopiert werden,

Beim Kopieren von einem dieser Standorte	Zu diesem Ort	DataSync kann kopieren
		werden die Dateimetadaten wiederhergestellt. Für die Wiederherstellung von Metadaten müssen dem NFS-Server erhöhte Berechtigungen gewährt werden. Weitere Informationen finden Sie unter Konfiguration von AWS DataSync Übertragungen mit einem NFS-Dateiserver.

Zwischen Amazon S3 und anderem Objektspeicher

Beim Kopieren zwischen diesen Speicherorten	DataSync kann kopieren
• Objektspeicher • Amazon S3	• Benutzerdefinierte Objektmetadaten • Objekt-Tags • Die folgenden systemdefinierten Objektmetadaten: • Content-Disposition • Content-Encoding • Content-Language • Content-Type Hinweis: DataSync kopiert bei einer ersten Übertragung Metadaten auf Systemebene für alle Objekte. Wenn Sie Ihre Aufgabe so konfigurieren, dass nur Daten übertragen werden, die sich geändert haben, DataSync werden bei nachfolgenden Übertragungen keine Systemmetadaten kopiert, es sei denn,
• Microsoft Azure Blob Storage • Amazon S3	

Beim Kopieren zwischen diesen Speicherorten	DataSync kann kopieren
	der Inhalt eines Objekts oder die Benutzermetadaten wurden ebenfalls geändert. DataSync kopiert keine anderen Objektmetadaten, wie z. B. Objektzugriffskontrolllisten (ACLs), frühere Objektversionen oder den Schlüssel „Zuletzt geändert“.

Zwischen Amazon S3 und HDFS

Beim Kopieren zwischen diesen Speicherorten	DataSync kann kopieren
• Hadoop Distributed File System (HDFS) • Amazon S3	Folgendes als Amazon S3 S3-Benutzermetadaten: • Zeitstempel für Datei- und Ordneränderungen • Zeitstempel für den Datei- und Ordnerzugriff (DataSync dies ist nur nach bestem Wissen möglich) • Benutzer-ID und Gruppen-ID • POSIX-Berechtigungen HDFS verwendet Zeichenfolgen, um den Besitz von Benutzern und Gruppen für Dateien und Ordner zu speichern, und nicht numerische Kennungen wie uid und gid.

Bei NFS-Übertragungen kopierte Metadaten

In der folgenden Tabelle wird beschrieben, welche Metadaten zwischen Speicherorten kopiert werden können, die das Network File System (NFS) verwenden.

Beim Kopieren zwischen diesen Speicherorten	DataSync kann kopieren
• NFS • Amazon EFS • Amazon FSx für Lustre • Amazon FSx für OpenZFS • Amazon FSx für NetApp ONTAP (mit NFS)	• Zeitstempel für Datei- und Ordneränderungen • Zeitstempel für den Datei- und Ordnerzugriff (DataSync dies ist nur nach bestem Wissen möglich) • Benutzer-ID (UID) und Gruppen-ID (GID) • POSIX-Berechtigungen

Metadaten, die bei SMB-Übertragungen kopiert wurden

In der folgenden Tabelle wird beschrieben, welche Metadaten zwischen Speicherorten kopiert werden DataSync können, die Server Message Block (SMB) verwenden.

Beim Kopieren zwischen diesen Speicherorten	DataSync kann kopieren
• SMB • Amazon FSx für Windows-Dateiserver • FSx für ONTAP (mit SMB)	• Dateizeitstempel: Zugriffszeit, Änderungszeit und Erstellungszeit • Sicherheits-ID (SID) des Dateibesitzers • Standarddateiattribute: schreibgeschützt (R), Archiv (A), System (S), versteckt (H), komprimiert (C), nicht inhaltsindiziert (I), verschlüsselt (E), temporär (T), offline (O) und spärlich (P) DataSync versucht, die Attribute Archiv (A), komprimiert (C), nicht kontextindexiert (I), Sparse (P) und temporär (T) nach bestem Wissen zu kopieren. Wenn diese Attribute nicht auf das Ziel angewendet werden, werden sie bei der Aufgabenüberprüfung ignoriert.

Beim Kopieren zwischen diesen Speicherorten	DataSync kann kopieren
	• Diskretionäre NTFS-Zugriffslisten (DACLS), mit denen festgelegt wird, ob Zugriff auf ein Objekt gewährt wird. • NTFS-Systemzugriffskontrolllisten (SACLs), die von Administratoren verwendet werden, um Zugriffsversuche auf ein geschütztes Objekt zu protokollieren. Hinweis: SACLs werden nicht kopiert, wenn Sie SMB Version 1.0 verwenden. Das Kopieren DACLS SACLs erfordert, dass dem Windows-Benutzer, der über SMB auf Ihren Standort DataSync zugreift, bestimmte Berechtigungen erteilt werden. Weitere Informationen finden Sie unter Erstellen eines Speicherorts für SMB, FSx für Windows File Server oder FSx für ONTAP (je nach Art des Speicherorts in Ihrer Übertragung).

Metadaten, die in anderen Übertragungsszenarien kopiert wurden

DataSync verarbeitet Metadaten beim Kopieren zwischen diesen Speichersystemen (von denen die meisten unterschiedliche Metadatenstrukturen haben) auf folgende Weise.

Beim Kopieren von einem dieser Speicherorte	An einen dieser Orte	DataSync kann kopieren
• SMB • FSx für Windows-Dateiserver • FSx für ONTAP (mit SMB)	• Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS) • Amazon S3	POSIX-Standard-Metadaten für alle Dateien und Ordner im Zielspeichersystem oder für Objekte im Ziel-S3-Bucket. Dieser Ansatz umfasst die Verwendung der standardm

Beim Kopieren von einem dieser Speicherorte	An einen dieser Orte	DataSync kann kopieren
	• Objektspeicher • Azure Blob Storage • NFS	äßigen POSIX-Benutzer-ID- und Gruppen-ID-Werte. Windows-basierte Metadaten (wie ACLs) werden nicht beibehalten.
• Objektspeicher • Amazon S3 • Azure Blob Storage	• Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS)	POSIX-Standard-Metadaten für die Zieldateien und -ordner. Dieser Ansatz umfasst die Verwendung der standardmäßigsten POSIX-Benutzer-ID- und Gruppen-ID-Werte.
• Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS)	• Azure Blob Storage	Folgendes als benutzerdefinierte Metadaten: • Zeitstempel für Datei- und Ordneränderungen • Zeitstempel für Datei- und Ordnerzugriffe (DataSync dies ist nur nach bestem Wissen möglich) • Benutzer-ID und Gruppen-ID • POSIX-Berechtigungen

Beim Kopieren von einem dieser Speicherorte	An einen dieser Orte	DataSync kann kopieren
• HDFS	• Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS)	• Zeitstempel für Datei- und Ordneränderungen • Zeitstempel für Datei- und Ordnerzugriffe (DataSync dies ist nur nach bestem Wissen möglich) • POSIX-Berechtigungen HDFS speichert den Besitz von Benutzern und Gruppen von Dateien und Ordnern als Zeichenketten und nicht als numerische Bezeichner (wie uid und gid). UID und GID Standardwerte für UID und GID werden auf das Zielsystem angewendet. Weitere Informationen finden Sie unter Verstehen, wann und wie DataSync POSIX-Standardmetadaten angewendet werden.

Beim Kopieren von einem dieser Speicherorte	An einen dieser Orte	DataSync kann kopieren
• Amazon S3 • Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für Windows-Dateiserver • FSx für ONTAP	• HDFS	Zeitstempel von Dateien und Ordnern vom Quellspeicherort. Der Besitzer der Datei oder des Ordners wird auf der Grundlage des HDFS-Benutzers oder Kerberos-Prinzips festgelegt, den Sie bei der Erstellung des HDFS-Übertragungsorts angegeben haben. Die Gruppenzuordnungskonfiguration auf dem Hadoop-Cluster bestimmt die Gruppe.
• Amazon S3 • Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS) • Objektspeicher • NFS • HDFS	• SMB • FSx für Windows-Dateiserver • FSx für ONTAP (mit SMB)	Zeitstempel von Dateien und Ordnern vom Quellspeicherort. Die Eigentümerschaft wird auf der Grundlage des Windows-Benutzers festgelegt, der für den DataSync Zugriff auf die Amazon FSx - oder SMB-Freigabe angegeben wurde. Die Berechtigungen werden aus dem übergeordneten Verzeichnis übernommen.
• Azure Blob Storage	• FSx für Windows-Dateiserver • FSx für ONTAP (mit SMB)	

Verstehen, wann und wie DataSync POSIX-Standardmetadaten angewendet werden

DataSync wendet standardmäßige POSIX-Metadaten in den folgenden Situationen an:

- Wenn die Quell- und Zielorte Ihrer Übertragung keine ähnlichen Metadatenstrukturen haben

- Wenn Metadaten am Quellort fehlen

In der folgenden Tabelle wird beschrieben, wie POSIX-Standardmetadaten bei diesen Arten von Übertragungen DataSync angewendet werden:

Quelle	Ziel	Dateiberechtigungen	Ordnerberechtigungen	Benutzerkennung (UID)	GID
• Amazon S3¹ • Objektspeicher¹ • Microsoft Azure Blob Storage¹	• Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS) • NFS	0755	0755	65534	65534
• SMB	• Amazon S3 • Objektspeicher • Amazon EFS • FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS) • NFS	0644	0755	65534	65534
• HDFS	• Amazon EFS	0644	0755	65534	65534

Quelle	Ziel	Dateiberechtigungen	Ordnerberechtigungen	Benutzerkennung (UID)	GID
	• FSx für Lustre • FSx für OpenZFS • FSx für ONTAP (mit NFS) • NFS				

¹ In Fällen, in denen die Objekte keine Metadaten haben, die zuvor von angewendet wurden. DataSync

Links und Verzeichnisse, die kopiert wurden von AWS DataSync

AWS DataSync behandelt Hardlinks, symbolische Links und Verzeichnisse je nach den Speicherorten, die an Ihrer Übertragung beteiligt sind, unterschiedlich.

Hard-Links

So werden Hardlinks in einigen gängigen Übertragungsszenarien DataSync behandelt:

- Bei der Übertragung zwischen einem NFS-Dateiserver FSx für Lustre, FSx für OpenZFS, FSx für ONTAP (mit NFS) und Amazon EFS werden Hardlinks beibehalten.
- Bei der Übertragung an Amazon S3 wird jede zugrunde liegende Datei, auf die ein Hardlink verweist, nur einmal übertragen. Bei inkrementellen Übertragungen werden separate Objekte in Ihrem S3-Bucket erstellt. Wenn ein Hardlink in Amazon S3 unverändert ist, wird er korrekt wiederhergestellt, wenn er auf einen NFS-Dateiserver, FSx für Lustre, für OpenZFS, FSx für ONTAP (mit NFS) oder das Amazon EFS-Dateisystem übertragen wird.
- Bei der Übertragung an Microsoft Azure Blob Storage, auf die ein Hardlink verweist, nur einmal übertragen. Bei inkrementellen Übertragungen werden separate Objekte in Ihrem Blob-Speicher erstellt, wenn die Quelle neue Verweise enthält. Bei der Übertragung von werden Hardlinks so DataSync übertragen Azure Blob Storage, als ob es sich um einzelne Dateien handeln würde.

- Bei der Übertragung zwischen einem SMB-Dateiserver, FSx für Windows File Server und FSx für ONTAP (mit SMB) werden Hardlinks nicht unterstützt. Wenn Sie in diesen Situationen DataSync auf Hardlinks stoßen, wird die Übertragungsaufgabe mit einem Fehler abgeschlossen. Weitere Informationen finden Sie in Ihren CloudWatch Protokollen.
- Bei der Übertragung auf HDFS werden Hardlinks nicht unterstützt. CloudWatch In den Protokollen werden diese Links als übersprungen angezeigt.

Symbolische Verknüpfungen

So werden symbolische Links in einigen gängigen Übertragungsszenarien DataSync behandelt:

- Bei der Übertragung zwischen einem NFS-Dateiserver FSx für Lustre, für OpenZFS, FSx FSx für ONTAP (mit NFS) und Amazon EFS werden symbolische Links beibehalten.
- Bei der Übertragung zu Amazon S3 wird der Linkzielpfad im Amazon S3 S3-Objekt gespeichert. Der Link wird korrekt wiederhergestellt, wenn er auf einen NFS-Dateiserver, FSx für Lustre, für OpenZFS, FSx FSx für ONTAP oder das Amazon EFS-Dateisystem übertragen wird.
- Bei der Übertragung an werden symbolische Azure Blob Storage Links nicht unterstützt. CloudWatch In den Protokollen werden diese Links als übersprungen angezeigt.
- Bei der Übertragung zwischen einem SMB-Dateiserver, FSx für Windows File Server und FSx für ONTAP (mit SMB) werden symbolische Links nicht unterstützt. DataSync überträgt keinen symbolischen Link selbst, sondern eine Datei, auf die durch den symbolischen Link verwiesen wird. Um doppelte Dateien zu erkennen und sie mit symbolischen Links zu deduplizieren, müssen Sie die Deduplizierung in Ihrem Zieldateisystem konfigurieren.
- Bei der Übertragung auf HDFS werden symbolische Links nicht unterstützt. CloudWatch In den Protokollen werden diese Links als übersprungen angezeigt.

Verzeichnisse

Im Allgemeinen werden Verzeichnisse bei der Übertragung zwischen Speichersystemen DataSync beibehalten. Dies ist in den folgenden Situationen nicht der Fall:

- Bei der Übertragung an Amazon S3 werden Verzeichnisse als leere Objekte dargestellt, die Präfixe haben und mit einem Schrägstrich (/) enden.
- Bei der Übertragung in ein Verzeichnis Azure Blob Storage ohne hierarchischen Namespace existieren keine Verzeichnisse. Was wie ein Verzeichnis aussieht, ist nur ein Teil eines Objektnamens.

Konfiguration des Umgangs mit Dateien, Objekten und Metadaten

Sie können konfigurieren, wie Ihre Dateien, Objekte und die zugehörigen Metadaten bei der Übertragung zwischen Speicherorten AWS DataSync behandelt werden.

Bei wiederkehrenden Übertragungen möchten Sie beispielsweise möglicherweise Dateien in Ihrem Ziel mit Änderungen in der Quelle überschreiben, um die Speicherorte synchron zu halten. Sie können Eigenschaften wie POSIX-Berechtigungen für Dateien und Ordner, mit Objekten verknüpfte Tags und Zugriffskontrolllisten (ACLs) kopieren.

Optionen für den Übertragungsmodus

Sie können konfigurieren, ob nur die Daten (einschließlich Metadaten) DataSync übertragen werden, die nach einer ersten Kopie geändert wurden, oder alle Daten bei jeder Ausführung der Aufgabe. Wenn Sie wiederkehrende Übertragungen planen, möchten Sie möglicherweise nur die Änderungen übertragen, die sich seit der letzten Ausführung der Aufgabe geändert haben.

Option in der Konsole	Option in der API	Description
Übertrage nur Daten, die sich geändert haben	TransferMode eingestellt auf CHANGED	Nach der ersten vollständigen Übertragung werden nur die Daten und Metadaten DataSync kopiert, die sich zwischen dem Quell- und dem Zielort unterscheiden.
Alle Daten übertragen	TransferMode eingestellt auf ALL	DataSync kopiert alles in der Quelle in das Ziel, ohne die Unterschiede zwischen den Speicherorten zu vergleichen.

Optionen für die Datei- und Objektverwaltung

Sie können einige Aspekte der DataSync Behandlung Ihrer Dateien oder Objekte am Zielort steuern. Sie DataSync können beispielsweise Dateien am Ziel löschen, die sich nicht in der Quelle befinden.

Option in der Konsole	Option in der API	Description
Behalte gelöschte Dateien	PreserveDeletedFiles	Gibt an, ob Dateien oder Objekte am Zielspeicherort DataSync verwaltet werden, die in der Quelle nicht vorhanden sind. Wenn Sie Ihre Aufgabe so konfigurieren, dass Objekte aus Ihrem Amazon S3 S3-Bucket gelöscht werden, fallen möglicherweise Gebühren für die Mindestspeicherdauer für bestimmte Speicherklassen an. Weitere Informationen hierzu finden Sie unter Überlegungen zur Speicherklassse bei Amazon S3 S3-Übertragungen.  Warning Sie können Ihre Aufgabe nicht so konfigurieren, dass Daten im Ziel gelöscht und gleichzeitig alle Daten übertragen werden. Wenn Sie alle Daten übertragen, wird Ihr Zielort DataSync nicht gescannt und Sie wissen nicht, was gelöscht werden soll.

Option in der Konsole	Option in der API	Description
Dateien überschreiben	OverwriteMode	Gibt an, ob DataSync Daten im Zielverzeichnis geändert werden, wenn sich die Quelldaten oder Metadaten geändert haben. Wenn Sie Ihre Aufgabe nicht so konfigurieren, dass Daten überschrieben werden, werden die Zieldaten auch dann nicht überschrieben, wenn sich die Quelldaten unterscheiden. Wenn Ihre Aufgabe Objekte überschreibt, fallen möglicherweise zusätzliche Gebühren für bestimmte Speicherklassen an (z. B. für das Abrufen oder vorzeitiges Löschen). Weitere Informationen hierzu finden Sie unter Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen.

Optionen für die Handhabung von Metadaten

DataSync kann Datei- und Objektmetadaten während einer Übertragung beibehalten. Welche Metadaten beibehalten DataSync werden können, hängt von den beteiligten Speichersystemen ab und davon, ob diese Systeme eine ähnliche Metadatenstruktur verwenden.

Stellen Sie vor der Konfiguration Ihrer Aufgabe sicher, dass Sie wissen, wie [Metadaten](#) und [spezielle Dateien](#) bei der Übertragung zwischen Ihrem Quell- und Zielspeicherort DataSync behandelt werden.

Important

DataSync unterstützt Übertragungen zu und von bestimmten Cloud-Speichersystemen von Drittanbietern wie Google Cloud Storage und IBM Cloud Object Storage, die

Systemmetadaten auf eine Weise verarbeiten, die nicht vollständig S3-kompatibel ist. Bei diesen Übertragungen wird DataSync versucht, Metadatenattribute wie `contentType`, `contentEncoding`, `contentTypeLanguage`, und nach bestem Wissen `cacheControl` zu kopieren. Wenn das Zielspeichersystem diese Attribute nicht anwendet, werden sie bei der Aufgabenüberprüfung ignoriert.

Option in der Konsole	Option in der API	Description
Besitz kopieren	Gid und Uid	Gibt an, ob der Besitz von POSIX-Dateien und -Ordern DataSync kopiert wird, z. B. die Gruppen-ID der Eigentümer der Datei und die Benutzer-ID des Besitzers der Datei.
Berechtigungen kopieren	PosixPermissions	Gibt an, ob POSIX-Berechtigungen für Dateien und Ordner von der Quelle zum Ziel DataSync kopiert werden.
Kopiert Zeitstempel	Atime und Mtime	Gibt an, ob die Zeitstempel-Metadaten von der Quelle zum Ziel DataSync kopiert werden. Erforderlich, wenn Sie eine Aufgabe mehr als einmal ausführen müssen.
Objekt-Tags kopieren	ObjectTags	Gibt an, DataSync ob die mit Ihren Objekten verknüpften Tags bei der Übertragung zwischen Objektspeichersystemen beibehalten werden.
Besitz kopieren DACLs, und SACLs	SecurityDescriptorCopyFlags gesetzt auf <code>OWNER_DACL_SACL</code>	DataSync kopiert Folgendes: • Der Objekteigentümer.

Option in der Konsole	Option in der API	Description
		• Diskretionäre NTFS-Zugriffslisten (DACLS), die festlegen, ob Zugriff auf ein Objekt gewährt wird. • NTFS-Systemzugriffskontrolllisten (SACLs), die von Administratoren verwendet werden, um Zugriffsversuche auf ein geschütztes Objekt zu protokollieren. Hinweis: SACLs werden nicht kopiert, wenn Sie SMB Version 1.0 verwenden. Das Kopieren DACLS SACLs erfordert, dass dem Windows-Benutzer, der über SMB auf Ihren Standort DataSync zugreift, bestimmte Berechtigungen erteilt werden. Weitere Informationen finden Sie unter Erstellen eines Speicherorts für SMB, FSx für Windows File Server oder FSx für ONTAP (je nach Art des Speicherorts in Ihrer Übertragung).

Option in der Konsole	Option in der API	Description
Besitz kopieren und DACLs	SecurityDescriptorCopyFlags eingestellt auf OWNER_DACL	DataSync kopiert Folgendes: • Der Objekteigentümer. • DACLs, die bestimmen, ob Zugriff auf ein Objekt gewährt werden soll. DataSync wird nicht kopiert SACLs , wenn Sie diese Option wählen.
Kopieren Sie nicht das Eigentum oder ACLs	SecurityDescriptorCopyFlags gesetzt auf NONE	DataSync kopiert keine Eigentums- oder Berechtigungsdaten. Die Objekte, DataSync die an Ihren Zielort schreiben, gehören dem Benutzer, dessen Anmeldeinformationen für den DataSync Zugriff auf das Ziel bereitgestellt wurden. Die Berechtigungen für Zielobjekte werden auf der Grundlage der auf dem Zielsystem konfigurierten Berechtigungen bestimmt.

Konfiguration der Optionen für die Handhabung von Dateien, Objekten und Metadaten

Sie können konfigurieren, wie Dateien, Objekte und Metadaten DataSync behandelt werden, wenn Sie Ihre Übertragungsaufgabe erstellen, bearbeiten oder starten.

Verwenden der DataSync -Konsole

In den folgenden Anweisungen wird beschrieben, wie Sie die Optionen für die Handhabung von Dateien, Objekten und Metadaten bei der Erstellung einer Aufgabe konfigurieren.

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.

2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Wählen Sie für den Übertragungsmodus eine der folgenden Optionen:
 - Nur Daten übertragen, die sich geändert haben
 - Alle Daten übertragen

Weitere Informationen zu diesen Optionen finden Sie unter [Optionen für den Übertragungsmodus](#).

5. Wählen Sie Gelöschte Dateien behalten DataSync, wenn Sie Dateien oder Objekte am Zielort behalten möchten, die in der Quelle nicht vorhanden sind.

Wenn Sie diese Option nicht wählen und Ihre Aufgabe Objekte aus Ihrem Amazon S3 S3-Bucket löscht, fallen möglicherweise Gebühren für die Mindestspeicherdauer für bestimmte Speicherklassen an. Weitere Informationen hierzu finden Sie unter [Überlegungen zur Speicherkategorie bei Amazon S3 S3-Übertragungen](#).

 Warning

Sie können diese Option nicht abwählen und die Option Alle Daten übertragen aktivieren. Wenn Sie alle Daten übertragen, wird Ihr Zielort DataSync nicht gescannt und Sie wissen nicht, was gelöscht werden soll.

6. Wählen Sie Dateien überschreiben, wenn Sie Daten am Zielort ändern DataSync möchten, wenn sich die Quelldaten oder Metadaten geändert haben.

Wenn Ihre Aufgabe Objekte überschreibt, fallen möglicherweise zusätzliche Gebühren für bestimmte Speicherklassen an (z. B. für das Abrufen oder vorzeitiges Löschen). Weitere Informationen hierzu finden Sie unter [Überlegungen zur Speicherkategorie bei Amazon S3 S3-Übertragungen](#).

Wenn Sie diese Option nicht wählen, werden die Zieldaten auch dann nicht überschrieben, wenn sich die Quelldaten unterscheiden.

7. Wählen Sie unter Übertragungsoptionen aus, wie Sie mit Metadaten umgehen DataSync möchten. Weitere Informationen zu diesen Optionen finden Sie unter [Optionen für die Handhabung von Metadaten](#).

 Important

Die Optionen, die Ihnen in der Konsole angezeigt werden, hängen von den Quell- und Zielorten Ihrer Aufgabe ab. Möglicherweise müssen Sie Zusätzliche Einstellungen erweitern, um einige dieser Optionen zu sehen.

- Besitz kopieren
- Berechtigungen kopieren
- Zeitstempel kopieren
- Objekt-Tags kopieren
- Besitz kopieren DACLS, und SACLS
- Besitz kopieren und DACLS
- Kopieren Sie nicht das Eigentum oder ACLs

Verwenden der DataSync API

Sie können Optionen für die Verarbeitung von Dateien, Objekten und Metadaten konfigurieren, indem Sie den `Options` Parameter mit einer der folgenden Operationen verwenden:

- [CreateTask](#)
- [StartTaskExecution](#)
- [UpdateTask](#)

Konfiguration, wie AWS DataSync die Datenintegrität überprüft wird

AWS DataSync Verwendet während einer Übertragung die Prüfsummenüberprüfung, um die Integrität der Daten zu überprüfen, die Sie zwischen Speicherorten kopieren. Sie können auch so konfigurieren DataSync , dass am Ende Ihrer Übertragung eine zusätzliche Überprüfung durchgeführt wird.

Optionen zur Datenüberprüfung

Verwenden Sie die folgenden Informationen, um zu entscheiden, ob und wie Sie diese zusätzlichen Prüfungen durchführen DataSync möchten.

Konsolenoption	API-Option	Description
Überprüfen Sie nur übertragene Daten (empfohlen)	VerifyMode eingestellt auf ONLY_FILES_TRANSFERRED	DataSync berechnet die Prüfsumme der übertragenen Daten (einschließlich Metadaten) am Quellspeicherort. Vergleicht am Ende Ihrer Übertragung diese Prüfsumme mit der Prüfsumme, die DataSync anhand derselben Daten am Ziel berechnet wurde. Wir empfehlen diese Option bei der Übertragung in die Speicherklassen S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive. Weitere Informationen finden Sie unter Überlegungen zur Speicherung bei Amazon S3 S3-Übertragungen.
Überprüfen Sie alle Daten	VerifyMode eingestellt auf POINT_IN_TIME_CONSISTENT	DataSync überprüft am Ende Ihrer Übertragung die gesamte Quelle und das Ziel, um sicherzustellen, dass beide Standorte vollständig synchronisiert sind.

Konsolenoption	API-Option	Description
		 Note Wird nicht unterstützt, wenn Ihre Aufgabe den erweiterten Modus verwendet. Wenn Sie ein Manifest verwenden, wird DataSync nur gescannt und verifiziert, was im Manifest aufgeführt ist. Sie können diese Option nicht verwenden, wenn Sie zu den Speicherklassen S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive übertragen. Weitere Informationen finden Sie unter Überlegungen zur Speicherung bei Amazon S3 S3-Übertragungen.
Überprüfen Sie die Daten nach der Übertragung nicht	VerifyMode eingestellt auf NONE	DataSync führt Datenintegritätsprüfungen nur während der Übertragung durch. Im Gegensatz zu anderen Optionen erfolgt am Ende Ihrer Übertragung keine zusätzliche Überprüfung.

Konfiguration der Datenüberprüfung

Sie können Optionen zur Datenüberprüfung konfigurieren, wenn Sie eine Aufgabe erstellen, eine Aufgabe aktualisieren oder eine Aufgabenausführung starten.

Verwenden der DataSync -Konsole

In den folgenden Anweisungen wird beschrieben, wie die Datenüberprüfungsoptionen beim Erstellen einer Aufgabe konfiguriert werden.

So konfigurieren Sie die Datenüberprüfung mithilfe der Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Wählen Sie für die Überprüfung eine der folgenden Optionen:
 - Überprüfen Sie nur übertragene Daten (empfohlen)
 - Überprüfen Sie alle Daten
 - Überprüfen Sie die Daten nach der Übertragung nicht

Verwenden der DataSync-API

Sie können konfigurieren, wie Daten DataSync überprüft werden, indem Sie den `VerifyMode` Parameter mit einer der folgenden Operationen verwenden:

- [CreateTask](#)
- [UpdateTask](#)
- [StartTaskExecution](#)

Legen Sie Bandbreitenlimits für Ihre Aufgabe fest AWS DataSync

Sie können Netzwerkbandbreitenbeschränkungen für Ihre AWS DataSync Aufgabe und jede ihrer Ausführungen konfigurieren.

 Note

Gilt nicht für [Aufgaben im erweiterten Modus](#).

Beschränken der Bandbreite für eine Aufgabe

Legen Sie ein Bandbreitenlimit fest, wenn Sie eine Aufgabe erstellen, bearbeiten oder starten.

Verwenden der DataSync-Konsole

In den folgenden Anweisungen wird beschrieben, wie Sie ein Bandbreitenlimit für Ihre Aufgabe konfigurieren, wenn Sie sie erstellen.

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Wählen Sie unter Bandbreitenlimit eine der folgenden Optionen:
 - Wählen Sie Verfügbare verwenden aus, um die gesamte verfügbare Netzwerkbandbreite für jede Aufgabenausführung zu verwenden.
 - Wählen Sie Bandbreitenlimit (MiB/s) festlegen und geben Sie die maximale Bandbreite ein, die Sie für jede Aufgabenausführung verwenden DataSync möchten.

Verwenden der API DataSync

Sie können das Bandbreitenlimit einer Aufgabe konfigurieren, indem Sie den BytesPerSecond Parameter mit einer der folgenden Operationen verwenden:

- [CreateTask](#)
- [UpdateTask](#)
- [StartTaskExecution](#)

Drosselung der Bandbreite für die Ausführung einer Aufgabe

Sie können das Bandbreitenlimit für die Ausführung einer laufenden Aufgabe oder für die Ausführung in der Warteschlange ändern.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>
2. Erweitern Sie im Navigationsbereich die Option Datenübertragung. Wählen Sie dann Aufgaben aus.
3. Wählen Sie die Aufgabe und dann Verlauf aus, um die Ausführungen der Aufgabe anzuzeigen.
4. Wählen Sie die Aufgabenausführung aus, die Sie ändern möchten, und klicken Sie dann auf Bearbeiten.
5. Wählen Sie im Dialogfeld eine der folgenden Optionen aus:
 - Wählen Sie Verfügbare verwenden, um die gesamte verfügbare Netzwerkbandbreite für die Ausführung der Aufgabe zu verwenden.
 - Wählen Sie Bandbreitenlimit (MiB/s) festlegen und geben Sie die maximale Bandbreite ein, die Sie für die Aufgabenausführung verwenden DataSync möchten.
6. Wählen Sie Änderungen speichern aus.

Das neue Bandbreitenlimit wird innerhalb von 60 Sekunden wirksam.

Verwenden der DataSync-API

Sie können das Bandbreitenlimit für die Ausführung einer laufenden oder in der Warteschlange befindlichen Aufgabe ändern, indem Sie den BytesPerSecond Parameter zusammen mit dem [UpdateTaskExecution](#) Vorgang verwenden.

Planen, wann Ihre AWS DataSync Aufgabe ausgeführt wird

Sie können einen AWS DataSync Taskplan für die regelmäßige Übertragung von Daten zwischen Speicherorten einrichten.

Wie funktioniert die DataSync Aufgabenplanung

Eine geplante DataSync Aufgabe wird mit einer von Ihnen angegebenen Häufigkeit ausgeführt, wobei das Mindestintervall 1 Stunde beträgt. Sie können einen Task-Zeitplan erstellen, indem Sie einen Cron- oder Rate-Ausdruck verwenden.

 Important

Sie können eine Aufgabe nicht so planen, dass sie in einem Intervall von weniger als einer Stunde ausgeführt wird.

Verwenden von Cron-Ausdrücken

Verwenden Sie Cron-Ausdrücke für Aufgabenpläne, die zu einer bestimmten Uhrzeit und an einem bestimmten Tag ausgeführt werden. So können Sie beispielsweise einen Task-Zeitplan konfigurieren AWS CLI , der jeden Sonntag und Mittwoch um 12:00 Uhr UTC läuft.

```
cron(0 12 ? * SUN,WED *)
```

Verwenden von Preisausdrücken

Verwenden Sie Ratenausdrücke für Aufgabenpläne, die in regelmäßigen Abständen ausgeführt werden, z. B. alle 12 Stunden. So können Sie beispielsweise einen Task-Zeitplan konfigurieren AWS CLI , der alle 12 Stunden ausgeführt wird:

```
rate(12 hours)
```

 Tip

Weitere Informationen zur Syntax von Cron- und Rate-Ausdrücken finden Sie im [EventBridge Amazon-Benutzerhandbuch](#).

Einen DataSync Aufgabenplan erstellen

Sie können mithilfe der DataSync Konsole oder der DataSync API planen AWS CLI, wie oft Ihre Aufgabe ausgeführt wird.

Mithilfe der DataSync Konsole

In den folgenden Anweisungen wird beschrieben, wie Sie beim Erstellen einer Aufgabe einen Zeitplan einrichten. Sie können den Zeitplan später ändern, wenn Sie die Aufgabe bearbeiten.

In der Konsole können Sie mit einigen Planungsoptionen die genaue Uhrzeit angeben, zu der Ihre Aufgabe ausgeführt wird (z. B. täglich um 22:30 Uhr). Wenn Sie für diese Optionen keine Uhrzeit angeben, wird Ihre Aufgabe zu dem Zeitpunkt ausgeführt, zu dem Sie die Aufgabe erstellen (oder aktualisieren).

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#)

4. Führen Sie für die Zeitplanhäufigkeit einen der folgenden Schritte aus:
 - Wählen Sie Nicht geplant, wenn Sie nicht möchten, dass Ihre Aufgabe nach einem Zeitplan ausgeführt wird.
 - Wählen Sie Stündlich und dann die Minute während der Stunde aus, in der Ihre Aufgabe ausgeführt werden soll.
 - Wählen Sie Täglich und geben Sie die UTC-Zeit ein, zu der Ihre Aufgabe ausgeführt werden soll.
 - Wählen Sie Wöchentlich und den Wochentag und geben Sie die UTC-Zeit ein, zu der die Aufgabe ausgeführt werden soll.
 - Wählen Sie Wochentage, wählen Sie einen oder mehrere bestimmte Tage und geben Sie die UTC-Zeit, zu der die Aufgabe ausgeführt werden soll, im Format HH:MM ein.
 - Wählen Sie Benutzerdefiniert und dann Cron-Ausdruck oder Rate-Ausdruck aus. Geben Sie Ihren Aufgabenplan mit einem Mindestintervall von 1 Stunde ein.

Verwenden Sie den AWS CLI

Sie können einen Zeitplan für Ihre DataSync Aufgabe erstellen, indem Sie den `--schedule` Parameter mit dem `start-task-execution` Befehl `create-taskupdate-task`, oder verwenden.

In den folgenden Anweisungen wird beschrieben, wie Sie dies mit dem `create-task` Befehl tun können.

1. Kopieren Sie den folgenden `create-task` Befehl:

```
aws datasync create-task \  
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/  
loc-12345678abcdefgh \\  
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/  
loc-abcdefgh12345678 \\  
  --schedule '{  
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)"   
  }'
```

2. Geben Sie für den `--source-location-arn` Parameter den Amazon-Ressourcennamen (ARN) des Standorts an, von dem Sie Daten übertragen.
3. Geben Sie für den `--destination-location-arn` Parameter den ARN des Standorts an, an den Sie Daten übertragen.
4. Geben Sie für den `--schedule` Parameter einen Cron- oder Rate-Ausdruck für Ihren Zeitplan an.

In diesem Beispiel `cron(0 12 ? * SUN,WED *)` legt der Cron-Ausdruck einen Task-Zeitplan fest, der jeden Sonntag und Mittwoch um 12:00 Uhr UTC ausgeführt wird.

5. Führen Sie den `create-task` Befehl aus, um Ihre Aufgabe mit dem Zeitplan zu erstellen.

Einen Task-Zeitplan pausieren DataSync

Es kann Situationen geben, in denen Sie Ihren DataSync Taskplan pausieren müssen.

Beispielsweise müssen Sie möglicherweise eine wiederkehrende Übertragung vorübergehend deaktivieren, um ein Problem mit Ihrer Aufgabe zu beheben oder Wartungsarbeiten an Ihrem Speichersystem durchzuführen.

DataSync könnte Ihren Taskplan aus den folgenden Gründen automatisch deaktivieren:

- Ihre Aufgabe schlägt wiederholt mit demselben Fehler fehl.
- Sie [deaktivieren einen AWS-Region](#), den Ihre Aufgabe verwendet.

Verwenden Sie die DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, und wählen Sie dann Aufgaben aus.

3. Wählen Sie die Aufgabe aus, für die Sie den Zeitplan unterbrechen möchten, und klicken Sie dann auf Bearbeiten.
4. Deaktivieren Sie für Zeitplan die Option Zeitplan aktivieren. Wählen Sie Änderungen speichern.

Verwenden des AWS CLI

1. Kopieren Sie den folgenden update-task Befehl:

```
aws datasync update-task \  
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh \  
  --schedule '{  
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)",  
    "Status": "DISABLED"  
  }'
```

2. Geben Sie für den --task-arn Parameter den ARN der Aufgabe an, für die Sie den Zeitplan unterbrechen möchten.
3. Gehen Sie für den --schedule Parameter wie folgt vor:
 - Geben Sie für ScheduleExpression einen Cron- oder Rate-Ausdruck für Ihren Zeitplan an.

Im Beispiel `cron(0 12 ? * SUN,WED *)` legt der Ausdruck einen Task-Zeitplan fest, der jeden Sonntag und Mittwoch um 12:00 Uhr UTC ausgeführt wird.
 - Geben Sie für DISABLED anStatus, dass der Taskplan angehalten werden soll.
4. Führen Sie den Befehl update-task aus.
5. Um den Zeitplan wieder aufzunehmen, führen Sie denselben update-task Befehl mit der Status Einstellung auf ausENABLED.

Überprüfen Sie den Status eines DataSync Task-Zeitplans

Sie können sehen, ob Ihr DataSync Taskplan aktiviert ist.

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, und wählen Sie dann Aufgaben aus.
3. Überprüfen Sie in der Spalte Zeitplan, ob der Zeitplan der Aufgabe aktiviert oder deaktiviert ist.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden `describe-task` Befehl:

```
aws datasync describe-task \  
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

2. Geben Sie für den `--task-arn` Parameter den ARN der Aufgabe an, zu der Sie Informationen benötigen.
3. Führen Sie den Befehl `describe-task` aus.

Sie erhalten eine Antwort mit Details zu Ihrer Aufgabe, einschließlich ihres Zeitplans. (Das folgende Beispiel konzentriert sich hauptsächlich auf die Konfiguration des Taskplans und zeigt keine vollständige `describe-task` Antwort.)

Das Beispiel zeigt, dass der Zeitplan der Aufgabe manuell deaktiviert wurde. Wenn der Zeitplan von deaktiviert ist DataSync SERVICE, wird eine Fehlermeldung angezeigt, die Ihnen hilft `DisabledReason` zu verstehen, warum die Aufgabe immer wieder fehlschlägt. Weitere Informationen finden Sie unter [???](#).

```
{  
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh",  
  "Status": "AVAILABLE",  
  "Schedule": {  
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)",  
    "Status": "DISABLED",  
    "StatusUpdateTime": 1697736000,  
    "DisabledBy": "USER",  
    "DisabledReason": "Manually disabled by user."  
  },  
  ...  
}
```

Ihre Aufgaben taggen AWS DataSync

Stichwörter sind Schlüssel-Wert-Paare, die Ihnen helfen, Ihre AWS DataSync Ressourcen zu verwalten, zu filtern und nach ihnen zu suchen. Sie können jeder DataSync Aufgabe und Aufgabenausführung bis zu 50 Tags hinzufügen.

Sie können beispielsweise eine Aufgabe für eine umfangreiche Datenmigration erstellen und die Aufgabe mit dem Schlüssel **Project** und dem Wert kennzeichnen **Large Migration**. Um die Migration weiter zu organisieren, könnten Sie eine Ausführung der Aufgabe mit dem Schlüssel **Transfer Date** und dem Wert kennzeichnen **May 2021** (nachfolgende Aufgabenausführungen könnten gekennzeichnet werden **June 2021**, **July 2021**, usw.).

Ihre Aufgabe taggen DataSync

Sie können Ihre DataSync Aufgabe nur markieren, wenn Sie die Aufgabe erstellen.

Verwenden der DataSync-Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Wählen Sie auf der Seite Einstellungen konfigurieren die Option Neues Tag hinzufügen aus, um Ihre Aufgabe zu taggen.

Verwenden Sie den AWS CLI

1. Kopieren Sie den folgenden create-task Befehl:

```
aws datasync create-task \
  --source-location-arn 'arn:aws:datsync:region:account-id:location/source-  
location-id' \
  --destination-location-arn 'arn:aws:datsync:region:account-  
id:location/destination-location-id' \
  --tags Key=tag-key,Value=tag-value
```

2. Geben Sie im Befehl die folgenden Parameter an:
 - `--source-location-arn`— Geben Sie den Amazon-Ressourcennamen (ARN) des Quellstandorts in Ihrer Übertragung an.
 - `--destination-location-arn`— Geben Sie bei Ihrer Übertragung den ARN des Zielorts an.

- `--tags`— Geben Sie die Tags an, die Sie auf die Aufgabe anwenden möchten.

Bei mehr als einem Tag trennen Sie jedes Schlüssel-Wert-Paar durch ein Leerzeichen.

3. (Optional) Geben Sie weitere Parameter an, die für Ihr Übertragungsszenario sinnvoll sind.

Eine Liste von `--options` finden Sie im Befehl [create-task](#).

4. Führen Sie den Befehl `create-task` aus.

Sie erhalten eine Antwort, in der die Aufgabe angezeigt wird, die Sie gerade erstellt haben.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

Um die Tags anzuzeigen, die Sie zu dieser Aufgabe hinzugefügt haben, können Sie den [list-tags-for-resource](#) Befehl verwenden.

Markieren Sie Ihre DataSync Aufgabenausführung

Sie können jeden Lauf Ihrer DataSync Aufgabe taggen.

Wenn Ihre Aufgabe bereits über Tags verfügt, sollten Sie Folgendes zur Verwendung von Tags bei Aufgabenausführungen beachten:

- Wenn Sie Ihre Aufgabe mit der Konsole starten, werden die von Benutzern erstellten Tags automatisch auf die Aufgabenausführung angewendet. Vom System erstellte Tags, die mit `aws:` beginnen, werden jedoch nicht angewendet.
- Wenn Sie Ihre Aufgabe mit der DataSync API oder starten AWS CLI, werden deren Tags nicht automatisch auf die Aufgabenausführung angewendet.

Verwenden der DataSync-Konsole

Um einer Aufgabenausführung Tags hinzuzufügen, zu bearbeiten oder zu entfernen, müssen Sie die Aufgabe mit übergeordneten Optionen starten.

1. Öffnen Sie die AWS DataSync Konsole unter. <https://console.aws.amazon.com/datasync/>

2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Aufgaben aus.
3. Wählen Sie die Aufgabe
4. Wählen Sie Start und anschließend eine der folgenden Optionen:
 - Mit Standardeinstellungen beginnen — Wendet alle mit Ihrer Aufgabe verknüpften Tags an.
 - Mit überschreibenden Optionen beginnen — Ermöglicht es Ihnen, Tags für diese spezielle Aufgabenausführung hinzuzufügen, zu bearbeiten oder zu entfernen.

Verwenden von AWS CLI

1. Kopieren Sie den folgenden `start-task-execution` Befehl:

```
aws datasync start-task-execution \  
  --task-arn 'arn:aws:datasync:region:account-id:task/task-id' \  
  --tags Key=tag-key,Value=tag-value
```

2. Geben Sie im Befehl die folgenden Parameter an:
 - `--task-arn`— Geben Sie den ARN der Aufgabe an, die Sie starten möchten.
 - `--tags`— Geben Sie die Tags an, die Sie auf diese spezielle Ausführung der Aufgabe anwenden möchten.

Bei mehr als einem Tag trennen Sie jedes Schlüssel-Wert-Paar durch ein Leerzeichen.

3. (Optional) Geben Sie weitere Parameter an, die für Ihre Situation sinnvoll sind.

Weitere Informationen finden Sie unter [start-task-execution](#)-Befehl.

4. Führen Sie den Befehl `start-task-execution` aus.

Sie erhalten eine Antwort, in der die Aufgabenausführung angezeigt wird, die Sie gerade gestartet haben.

```
{  
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:123456789012:task/task-  
  abcdef01234567890"  
}
```

Um die Tags anzuzeigen, die Sie zu dieser Aufgabe hinzugefügt haben, können Sie den [list-tags-for-resource](#) Befehl verwenden.

Eine Aufgabe zur Übertragung Ihrer Daten starten

Sobald Sie Ihre AWS DataSync Übertragungsaufgabe erstellt haben, können Sie mit dem Verschieben von Daten beginnen. Jede Ausführung einer Aufgabe wird als Aufgabenausführung bezeichnet. Hinweise dazu, was bei der Ausführung einer Aufgabe passiert, finden Sie unter [Wie werden Dateien, Objekte und Verzeichnisse DataSync übertragen](#).

Important

Wenn Sie planen, Daten zu oder von einem Amazon S3 S3-Standort zu übertragen, lesen Sie zunächst, [wie sich dies auf Ihre S3-Anforderungsgebühren auswirken DataSync kann](#), sowie auf der [DataSync Preisseite](#).

Starten Sie Ihre Aufgabe

Sobald Sie Ihre Aufgabe erstellt haben, können Sie sofort mit dem Verschieben von Daten beginnen.

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Aufgaben aus.
3. Wählen Sie die Aufgabe aus, die Sie ausführen möchten.

Stellen Sie sicher, dass die Aufgabe den Status Verfügbar hat. Sie können auch mehrere Aufgaben auswählen.

4. Wählen Sie Aktionen und dann eine der folgenden Optionen:
 - Start — Führt die Aufgabe aus (oder Aufgaben, falls Sie mehrere ausgewählt haben).
 - Mit überschreibenden Optionen beginnen — Ermöglicht es Ihnen, einige Ihrer Aufgabeneinstellungen zu ändern, bevor Sie mit dem Verschieben von Daten beginnen. Wenn Sie bereit sind, wählen Sie Start.
5. Wählen Sie Ausführungsdetails anzeigen, um Details zur Ausführung der laufenden Aufgabe anzuzeigen.

Verwenden Sie den AWS CLI

Um Ihre DataSync Aufgabe zu starten, müssen Sie nur den Amazon-Ressourcennamen (ARN) der Aufgabe angeben, die Sie ausführen möchten. Hier ist ein `start-task-execution` Beispielbefehl:

```
aws datasync start-task-execution \  
  --task-arn 'arn:aws:datasync:region:account-id:task/task-id'
```

Im folgenden Beispiel wird eine Aufgabe mit einigen Einstellungen gestartet, die sich von den Standardeinstellungen der Aufgabe unterscheiden:

```
aws datasync start-task-execution \  
  --override-options VerifyMode=NONE,OverwriteMode=NEVER,PosixPermissions=NONE
```

Der Befehl gibt einen ARN für Ihre Aufgabenausführung zurück, der dem folgenden Beispiel ähnelt:

```
{  
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:209870788375:task/  
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"  
}
```

Note

Jeder Agent kann jeweils eine einzelne Aufgabe ausführen.

Verwenden der DataSync API

Sie können Ihre Aufgabe mithilfe der [StartTaskExecution](#) Operation starten. Verwenden Sie den [DescribeTaskExecution](#) Vorgang, um Details zur Ausführung der laufenden Aufgabe abzurufen.

Nach dem Start können Sie den [Status der Aufgabenausführung überprüfen](#), während Ihre Daten DataSync kopiert werden. Sie können bei Bedarf auch [die Bandbreite der Aufgabenausführung drosseln](#).

Status der Aufgabenausführung

Wenn Sie eine DataSync Aufgabe starten, werden Ihnen möglicherweise diese Status angezeigt. (Der [Status von Aufgaben](#) unterscheidet sich vom Status der Aufgabenausführung.)

Status der Konsole	API-Status	Beschreibung
In der Warteschlange	QUEUED	Eine weitere Aufgabenausführung läuft und verwendet denselben DataSync Agenten. Weitere Informationen finden Sie unter Wissen Sie, wann sich Ihre Aufgabe in der Warteschlange befindet.
Wird gestartet	LAUNCHING	DataSync initialisiert die Ausführung der Aufgabe. Dieser Status vergeht normalerweise schnell, kann aber bis zu ein paar Minuten dauern.
Gestartet	LAUNCHED	DataSync hat die Ausführung der Aufgabe gestartet.
Schalten Sie die &Snowball;-Appliance ein, indem Sie auf den Ein-/Aus-Schalter über dem E-Ink-Display drücken.	PREPARING	DataSync bestimmt, welche Daten übertragen werden sollen. Die Vorbereitung kann nur wenige Minuten, einige Stunden oder sogar länger dauern, abhängig von der Anzahl der Dateien, Objekte oder Verzeichnisse an beiden Speicherorten und davon, wie Sie Ihre Aufgabe konfigurieren. Wie die Vorbereitung funktioniert, hängt auch von Ihrem Aufgabenmodus ab. Weitere Informationen finden Sie unter Wie wird Ihre Datenübertragung DataSync vorbereitet.
Übertragung	TRANSFERRING	DataSync führt die eigentliche Datenübertragung durch.
Wird überprüft	VERIFYING	DataSync überprüft die Integrität Ihrer Daten am Ende der Übertragung.
Herzlichen Glückwunsch	SUCCESS	Die Ausführung der Aufgabe war erfolgreich.
Abbrechen	CANCELLING	Die Ausführung der Aufgabe wird gerade abgebrochen.
Fehler	ERROR	Die Ausführung der Aufgabe ist fehlgeschlagen.

Wissen Sie, wann sich Ihre Aufgabe in der Warteschlange befindet

Wenn Sie mehrere Aufgaben ausführen (z. B. wenn Sie [einen großen Datensatz übertragen](#)), werden die Aufgaben DataSync möglicherweise in eine Warteschlange gestellt, sodass sie nacheinander ausgeführt werden (first in, first out). Einige Beispiele dafür, wann dies passiert, sind:

- Sie führen verschiedene Aufgaben aus, die denselben DataSync Agenten verwenden. Sie können zwar denselben Agenten für mehrere Aufgaben verwenden, ein Agent kann jedoch jeweils nur eine Aufgabe ausführen.
- Eine Aufgabenausführung ist im Gange und Sie starten weitere Ausführungen derselben Aufgabe mithilfe verschiedener [Filter](#) oder [Manifeste](#).

In jedem Beispiel beginnen die Aufgaben in der Warteschlange erst, wenn die Aufgabe, die vor ihnen liegt, beendet ist.

Die Ausführung Ihrer Aufgabe wird abgebrochen

Sie können jede Ausführung von laufenden Aufgaben oder DataSync Aufgaben in der Warteschlange beenden.

Um eine Aufgabenausführung mithilfe der Konsole abubrechen

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Aufgaben aus.
3. Wählen Sie die Task-ID für die laufende Aufgabe aus, die Sie überwachen möchten.

Der Aufgabenstatus sollte „Wird ausgeführt“ lauten.

4. Wählen Sie Verlauf, um die Ausführungen der Aufgabe anzuzeigen.
5. Wählen Sie die Aufgabenausführung aus, die Sie beenden möchten, und klicken Sie dann auf Beenden.
6. Wählen Sie im Dialogfeld die Option Beenden aus.

Informationen zum Abbrechen einer laufenden oder in der Warteschlange befindlichen Aufgabe mithilfe der DataSync API finden Sie unter [CancelTaskExecution](#).

Automatisches Abbrechen von hängengebliebenen Aufgaben

Manchmal kann die Ausführung einer laufenden DataSync Aufgabe hängen bleiben.

Überwachung Ihrer AWS DataSync Überweisungen

Die Überwachung ist wichtig, um die Zuverlässigkeit und Leistung Ihrer AWS DataSync Transferaktivitäten aufrechtzuerhalten. Wir empfehlen Ihnen, Überwachungsdaten zu sammeln, damit Sie etwaige Fehler leichter debuggen können. Bevor Sie mit der Überwachung beginnen DataSync, sollten Sie jedoch einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen werden überwacht?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungstools werden verwendet?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

AWS stellt verschiedene Dienste und Tools für die Überwachung bereit DataSync. Sie können einige davon so konfigurieren, dass sie die Überwachung für Sie übernehmen, andere erfordern jedoch manuelle Eingriffe. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

Themen

- [Leistungsindikatoren für die Datenübertragung verstehen](#)
- [Überwachung von Datenübertragungen mit CloudWatch Amazon-Metriken](#)
- [Überwachen Sie Ihre Datenübertragungen mit Aufgabenberichten](#)
- [Überwachung von Datenübertragungen mit Amazon CloudWatch Logs](#)
- [AWS DataSync API-Aufrufe protokollieren mit AWS CloudTrail](#)
- [Überwachung von Ereignissen mithilfe von Amazon EventBridge](#)
- [Überwachung AWS DataSync mit manuellen Tools](#)

Leistungsindikatoren für die Datenübertragung verstehen

Wenn Sie [eine Aufgabe starten](#), werden AWS DataSync Leistungsindikatoren angezeigt, anhand derer Sie die Leistung und den Fortschritt Ihrer Datenübertragung verfolgen können.

Verwenden Sie die folgenden Informationen, um zu verstehen, wofür die einzelnen Leistungsindikatoren stehen. Sie können sich diese Leistungsindikatoren in der DataSync Konsole oder in einer [DescribeTaskExecution](#) Antwort ansehen. Einige Leistungsindikatoren sind nicht in jedem [Aufgabenmodus](#) verfügbar.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
–	BytesWritten	Verbessert, Basic	Die Anzahl der logischen Byte, die DataSync tatsächlich an den Zielspeicherort schreiben.
Datendurchsatz	–	Verbessert, Einfach	Die Geschwindigkeit, mit der logische Bytes an den Zielspeicherort DataSync geschrieben werden. Wenn Sie verwenden DescribeTaskExecution, hängt die Berechnung dieses Zählers von Ihrem Aufgabenmodus ab: • Verbesserter Modus: Dividiere BytesWritten durch TotalDuration • Basismodus: Dividiere BytesWritten durch TransferDuration

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Übertragene Daten	BytesTransferred	Verbessert, Basic	Die Anzahl der Byte, die vor der Komprimierung an das Netzwerk DataSync gesendet werden (sofern eine Komprimierung möglich ist). Die Anzahl der über das Netzwerk übertragenen Byte finden Sie im Zähler für Netzwerkdurchsatz (in der Konsole) oder BytesCompressed (im DescribeTaskExecution).

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Aus dem Ziel gelöscht	FilesDeleted	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die an Ihrem Zielort DataSync tatsächlich gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden: • Aus Ziel gelöscht wird nicht in der Konsole angezeigt. • FilesDeleted zeigt immer einen Wert von 0.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Aus dem Ziel gelöscht	FilesDeleted , FoldersDeleted	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die an Ihrem Zielort DataSync tatsächlich gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden: • Aus Ziel gelöscht wird nicht in der Konsole angezeigt. • FilesDeleted und zeigt FoldersDeleted immer einen Wert von 0.
–	Estimated BytesTransferred	Verbessert, Einfach	Die Anzahl der logischen Byte, die DataSync voraussichtlich in den Zielspeicherort geschrieben werden.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
–	EstimatedFilesToDelete	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die DataSync voraussichtlich an Ihrem Zielort gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden, ist der Wert immer 0.
–	EstimatedFilesToDelete, EstimatedFoldersToDelete	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die DataSync voraussichtlich an Ihrem Zielort gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden, ist der Wert immer 0.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
–	EstimatedFilesToTransfer	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die DataSync voraussichtlich über das Netzwerk übertragen werden. Dieser Wert wird während der DataSync Vorbereitung der Übertragung berechnet. Wie dieser Wert berechnet wird, hängt hauptsächlich vom verwendeten Übertragungsmodus ab: • Wenn der Übertragungsmodus so eingestellt ist, dass nur Daten übertragen werden, die sich geändert haben: Die Berechnung basiert auf dem Vergleich des Inhalts der Quell- und Zielspeicherorte und der Bestimmung der Differenz,

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			die übertragen werden muss. Der Unterschied kann Folgendes beinhalten: • Alles, was am Quellspeicherort hinzugefügt oder geändert wurde. • Alles, was sich an beiden Speicheroorten befindet und nach einer ersten Übertragung am Ziel geändert wurde (es sei denn, Sie konfigurieren Ihre Aufgabe so, dass Daten im Ziel nicht überschrieben werden). • Die Anzahl der Elemente, die DataSync voraussichtlich gelöscht werden (wenn Sie Ihre Aufgabe so konfigurieren, dass Daten im Ziel gelöscht werden).

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			Wenn der Übertragungsmodus so eingestellt ist, dass alle Daten übertragen werden: Die Berechnung basiert nur auf den Elementen, die DataSync am Quellspeicherort gefunden wurden.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
–	EstimatedFilesToTransfer , EstimatedFoldersToTransfer	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die DataSync voraussichtlich über das Netzwerk übertragen werden. Dieser Wert wird während der DataSync Vorbereitung der Übertragung berechnet. Wie dieser Wert berechnet wird, hängt hauptsächlich vom verwendeten Übertragungsmodus ab: • Wenn der Übertragungsmodus so eingestellt ist, dass nur Daten übertragen werden, die sich geändert haben: Die Berechnung basiert auf dem Vergleich des Inhalts der Quell- und Zielspeicherorte und der Bestimmung

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			der Differenz, die übertragen werden muss. Der Unterschied kann Folgendes beinhalten: • Alles, was am Quellspeicherort hinzugefügt oder geändert wurde. • Alles, was sich an beiden Speicheroorten befindet und nach einer ersten Übertragung am Ziel geändert wurde (es sei denn, Sie konfigurieren Ihre Aufgabe so, dass Daten im Ziel nicht überschrieben werden). • Wenn der Übertragungsmodus so eingestellt ist, dass alle Daten übertragen werden: Die Berechnung basiert nur auf den Elementen, die am DataSync Quellspei

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			cherort gefunden wurden.
Dateidurchsatz	–	Verbessert, Basic	Die Geschwindigkeit, mit der Dateien, Objekte und Verzeichnisse über das Netzwerk DataSync übertragen werden. Wenn Sie verwenden DescribeTaskExecution, hängt die Berechnung dieses Zählers von Ihrem Aufgabenmodus ab: • Verbesserter Modus: Dividiere FilesTransferred durch TotalDuration • Basismodus: Dividiere FilesTransferred durch TransferDuration

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
–	FilesFailed , FoldersFailed	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die DataSync während der Ausführung der Aufgabe nicht vorbereitet, übertragen, überprüft und gelöscht werden konnten. Falls Fehler auftreten, können Sie diese zusammen mit den Zählern „Vorbereitet“, „Übertragen“, „Übersprungen“ und „Von der Zielkonsole gelöscht“ sehen.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
An der Quelle aufgeführt	FilesListed.AtSource, FoldersListed.AtSource	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die an DataSync Ihrem Quellspeicherort gefunden wurden. • DataSync Listet bei einem Manifest nur auf, was in Ihrem Manifest enthalten ist (und nicht alles, was sich in Ihrem Quellverzeichnis befindet). • Bei einem Include-Filter wird nur das DataSync aufgelistet, was dem Filter an Ihrem Quellspeicherort entspricht. • DataSync Listet bei einem Ausschlussfilter alles auf, was sich an Ihrem Quellstandort befindet, bevor der Filter angewendet wird.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
–	FilesListed.AtDestinationForDelete , FoldersListed.AtDestinationForDelete	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die DataSync an Ihrem Zielort gefunden wurden. Dieser Zähler gilt nur, wenn Sie Ihre Aufgabe so konfigurieren, dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Netzwerkdurchsatz *	BytesCompressed	Verbessert, Basic	Die Anzahl der physischen Byte, die nach der Komprimierung über das Netzwerk DataSync übertragen werden (sofern eine Komprimierung möglich ist). Diese Zahl ist in der Regel geringer als die übertragenen Daten (in der Konsole) oder BytesTransferred (in DescribeTaskExecution), es sei denn, die Daten sind nicht komprimierbar. * Im erweiterten Modus wird der Netzwerkdurchsatz nicht in der Konsole angezeigt.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Prozent komprimiert	–	Verbessert, Einfach	Der Prozentsatz der Übertragungsdaten, die vor dem Senden über das Netzwerk DataSync komprimiert wurden. Wenn Sie verwenden DescribeTaskExecution, können Sie diesen Zähler mit berechnen1 - BytesCompressed / BytesWritten .

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Vorbereitet	FilesPrepared , FoldersPrepared	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die nach dem Vergleich Ihrer Quell- und Zielverzeichnisse übertragen DataSync werden sollen. In der Konsole kann Ihnen dieser Zähler auch die Anzahl der Objekte anzeigen, die bei der Vorbereitung DataSync übersprungen wurden. Weitere Informationen finden Sie unter Wie wird Ihre Datenübertragung DataSync vorbereitet. Dieser Zähler ist nicht anwendbar, wenn Sie Ihre Aufgabe so konfigurieren, dass alle Daten übertragen werden. In diesem Szenario wird alles von der Quelle zum Ziel DataSync kopiert, ohne die Unterschiede zwischen den

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			Standorten zu vergleichen.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Verarbeitungsrate	–	Verbessert, Einfach	Die Geschwindigkeit, mit der Dateien, Objekte und Verzeichnisse an Ihrem Quellspeicherort DataSync gelesen werden. Die Verarbeitungsrate basiert auf mehreren CloudWatch Messwerten. Die genauen Metriken hängen vom verwendeten Aufgabenmodus ab. Verbesserter Modus: - FilesListedSource - FilesPrepared - FilesTransferred - FilesVerified Basismodus: - FilesPreparedSource - FilesPreparedDestination

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			- FilesTransferred - FilesVerifiedSource - FilesVerifiedDestination
Verbleibend	–	Basic	Die verbleibende Anzahl von Dateien, Objekten und Verzeichnissen, die DataSync voraussichtlich über das Netzwerk übertragen werden. Wenn Sie verwenden DescribeTaskExecution, können Sie diesen Zähler berechnen, indem Sie von <code>subtransferFilesTransferred</code> <code>EstimatedFilesToTransfer</code> subtrahieren.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
* Übersprungen	FilesSkipped	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die bei der Übertragung DataSync übersprungen werden.
–	FilesSkipped , FoldersSkipped	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die bei der Übertragung DataSync übersprungen werden. Übersprungene Elemente werden in den Zähler „Vorbereitet“ aufgenommen, wenn nur die Daten übertragen werden, die sich geändert haben, oder im Zähler „Übertrag“, wenn alle Daten übertragen werden.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Übertragt	FilesTransferred	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die über das Netzwerk DataSync übertragen werden. Dieser Wert wird während der Ausführung der Aufgabe regelmäßig aktualisiert, wenn etwas aus der Quelle gelesen und über das Netzwerk gesendet wird. Wenn DataSync etwas nicht übertragen werden kann, kann dieser Wert kleiner als <code>EstimatedFilesToTransfer</code> oder <code>seinEstimatedFoldersToTransfer</code>. In einigen Fällen kann dieser Wert auch größer als <code>EstimatedFilesToTransfer</code> oder <code>seinEstimatedFoldersToTransfer</code>. Dieser

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			Leistungsindikator ist für einige Standorttypen implementierungsspezifisch. Verwenden Sie ihn also nicht als exakten Hinweis darauf, was übertragen wird, oder um die Ausführung Ihrer Aufgabe zu überwachen.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Übertragt	FilesTransferred , FoldersTransferred	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die über das Netzwerk DataSync übertragen werden. Dieser Wert wird während der Ausführung der Aufgabe regelmäßig aktualisiert, wenn etwas aus der Quelle gelesen und über das Netzwerk gesendet wird. Wenn DataSync etwas nicht übertragen werden kann, kann dieser Wert kleiner als EstimatedFilesToTransfer oder seinEstimatedFoldersToTransfer . In einigen Fällen kann dieser Wert auch größer als EstimatedFilesToTransfer oder seinEstimatedFoldersToTransfer . Dieser

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
			Leistungsindikator ist für einige Standorttypen implementierungsspezifisch. Verwenden Sie ihn also nicht als exakten Hinweis darauf, was übertragen wird, oder um die Ausführung Ihrer Aufgabe zu überwachen.
Verifiziert	FilesVerified	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die während Ihrer Übertragung DataSync überprüft werden. Wenn Sie Ihre Aufgabe so konfigurieren, dass nur übertragene Daten überprüft werden, werden in einigen Situationen Verzeichnisse oder Dateien oder Objekte, die DataSync nicht übertragen werden können, nicht überprüft.

Konsole	DescribeTaskExecution	Unterstützung für den Aufgabenmodus	Description
Verifiziert	FilesVerified , FoldersVerified	Verbessert	Die Anzahl der Dateien oder Objekte und Verzeichnisse, die während der Übertragung DataSync überprüft werden.

Überwachung von Datenübertragungen mit CloudWatch Amazon-Metriken

Amazon CloudWatch stellt Kennzahlen zur Verfügung, mit denen Sie die DataSync Übertragungsleistung verfolgen und Probleme mit Ihrer Übertragungsaufgabe beheben können.

Sie können die AWS DataSync Übertragungsleistung mithilfe von CloudWatch Amazon-Metriken überwachen. DataSync Metriken werden automatisch CloudWatch in 5-Minuten-Intervallen gesendet (unabhängig davon, wie Sie die [Protokollierung konfigurieren](#)). Die Metriken werden für einen Zeitraum von 15 Monaten aufbewahrt.

Um CloudWatch Kennzahlen für zu sehen DataSync, können Sie die folgenden Tools verwenden:

- Die CloudWatch Konsole
- Die CloudWatch CLI
- Die CloudWatch API
- Die DataSync Konsole (auf der Detailseite der Aufgabenausführung)

Weitere Informationen finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

CloudWatch Metriken für DataSync

DataSync Metriken verwenden den `aws/datasync` Namespace und stellen Metriken für die folgenden Dimensionen bereit:

- AgentId— Die eindeutige ID des Agenten (falls Ihre Aufgabe einen Agenten verwendet).
- TaskId— Die eindeutige ID der Aufgabe. Er hat die Form task-*01234567890abcdef*.

Der aws/datasync-Namespace enthält die folgenden Metriken. Einige Metriken sind nicht in jedem [Aufgabenmodus](#) verfügbar.

CloudWatch Metrik	Unterstützung für den Aufgabenmodus	Beschreibung
BytesCompressed	Basic	Die Anzahl der physischen Byte, die nach der Komprimierung über das Netzwerk DataSync übertragen werden (sofern eine Komprimierung möglich ist). Diese Zahl ist in der Regel geringer als, BytesTransferred sofern die Daten nicht komprimierbar sind. Einheit: Byte
BytesPreparedDestination	Basic	Die Anzahl der logischen Byte, die am Zielspeicherort DataSync vorbereitet werden. Einheit: Byte
BytesPreparedSource	Basic	Die Anzahl der logischen Byte, die am Quellspeicherort DataSync vorbereitet werden. Einheit: Byte
BytesTransferred	Basic	Die Anzahl der Byte, die vor der Komprimierung an das Netzwerk DataSync gesendet werden (sofern eine Komprimierung möglich ist). Die Anzahl der über das Netzwerk übertragenen Byte finden Sie in der BytesCompressed Metrik. Einheit: Byte
BytesVerifiedDestination	Basic	Die Anzahl der logischen Byte, die am Zielstandort DataSync verifiziert werden.

CloudWatch Metrik	Unterstützung für den Aufgabenmodus	Beschreibung
		Einheit: Byte
BytesVerifiedSource	Basic	Die Anzahl der logischen Byte, die am DataSync Quellspeicherort verifiziert werden. Einheiten: Byte
BytesWritten	Verbessert, Einfach	Die Anzahl der logischen Byte, die in den Zielspeicherort DataSync geschrieben werden. Einheit: Byte
FilesDeleted	Verbessert, Einfach	Die Anzahl der Dateien, Objekte und Verzeichnisse, die an Ihrem Zielort DataSync gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden , ist der Wert immer 0. Einheit: Anzahl
FilesListedSource	Verbessert	Die Anzahl der Objekte, die DataSync an Ihrem Quellort gefunden wurden. Einheit: Anzahl

CloudWatch Metrik	Unterstützung für den Aufgabenmodus	Beschreibung
FilesPrepared	Verbessert	Die Anzahl der Objekte, DataSync die nach dem Vergleich Ihrer Quell- und Zielorte zu übertragen versuchen. Weitere Informationen finden Sie unter Wie wird Ihre Datenübertragung DataSync vorbereitet. Diese Metrik ist nicht anwendbar, wenn Sie Ihre Aufgabe so konfigurieren, dass alle Daten übertragen werden. In diesem Szenario wird alles von der Quelle zum Ziel DataSync kopiert, ohne die Unterschiede zwischen den Speicherorten zu vergleichen. Einheit: Anzahl
FilesPreparedDestination	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die am Zielort DataSync vorbereitet werden. Einheit: Anzahl
FilesPreparedSource	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die am Quellspeicherort DataSync vorbereitet werden. Einheit: Anzahl
FilesSkipped	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die bei der Übertragung DataSync übersprungen werden. Einheit: Anzahl

CloudWatch Metrik	Unterstützung für den Aufgabenmodus	Beschreibung
FilesTransferred	Verbessert, Einfach	Die Anzahl der Dateien, Objekte und Verzeichnisse, die über das Netzwerk DataSync übertragen werden. Dieser Wert wird während der Ausführung der Aufgabe regelmäßig aktualisiert, wenn etwas aus der Quelle gelesen und über das Netzwerk gesendet wird.  Note Dieser Wert kann niedriger sein als EstimatedFilesToTransfer in einer DescribeTaskExecution Antwort, wenn DataSync etwas nicht übertragen werden kann. In einigen Fällen kann dieser Wert auch größer als seinEstimatedFilesToTransfer sein. Diese Metrik ist für einige Standorttypen implementierungsspezifisch. Verwenden Sie sie daher nicht als exakte Angabe dafür, was übertragen wurde, oder um die Ausführung Ihrer Aufgabe zu überwachen. Einheit: Anzahl
FilesVerified	Verbessert	Die Anzahl der Objekte, die während Ihrer Übertragung DataSync verifiziert werden. Einheit: Anzahl
FilesVerifiedDestination	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die am Zielort DataSync überprüft werden. Einheit: Anzahl

CloudWatch Metrik	Unterstützung für den Aufgabenmodus	Beschreibung
FilesVerifiedSource	Basic	Die Anzahl der Dateien, Objekte und Verzeichnisse, die am DataSync Quellspeicherort überprüft werden. Einheit: Anzahl

Überwachen Sie Ihre Datenübertragungen mit Aufgabenberichten

Aufgabenberichte enthalten detaillierte Informationen darüber, welche AWS DataSync Versuche während der Ausführung einer Aufgabe übertragen, übersprungen, verifiziert und gelöscht werden. Weitere Informationen finden Sie unter [Wie werden Dateien, Objekte und Verzeichnisse DataSync übertragen](#).

Aufgabenberichte werden im JSON-Format generiert. Sie können den Detaillierungsgrad Ihrer Berichte anpassen:

- [Aufgabenberichte, die nur zusammenfassend](#) sind, enthalten die erforderlichen Informationen zur Ausführung Ihrer Aufgabe, z. B. wie viele Dateien übertragen wurden und ob die Datenintegrität dieser Dateien überprüft werden konnte.
- [Standardmäßige Aufgabenberichte](#) enthalten eine Zusammenfassung sowie detaillierte Berichte, in denen alle Dateien, Objekte oder Ordner aufgeführt sind, die DataSync übertragen, übersprungen, überprüft und gelöscht werden sollen. Bei einem Standardaufgabenbericht können Sie auch die [Berichtsebene](#) so festlegen, dass nur die Fehler oder die Erfolge und Fehler der Aufgabenausführung angezeigt werden.

Anwendungsfälle

Im Folgenden finden Sie einige Situationen, in denen Aufgabenberichte Ihnen helfen können, Ihre Datenübertragungen zu überwachen und zu prüfen:

- Identifizieren Sie bei der Migration von Millionen von Dateien schnell Dateien, bei denen DataSync Probleme bei der Übertragung auftreten.
- Überprüfen Sie chain-of-custody die Prozesse für Ihre Dateien.

Aufgabenberichte nur zusammenfassend

Ein Bericht, der nur eine Zusammenfassung der Ausführung einer Aufgabe darstellt, enthält die folgenden Details:

- Der AWS-Konto , der die Aufgabenausführung ausgeführt hat
- Die Quell- und Zielorte
- Die Gesamtzahl der Dateien, Objekte und Ordner, die übersprungen, übertragen, verifiziert und gelöscht wurden
- Die Gesamtzahl der übertragenen Byte (logisch und physisch)
- Wenn die Ausführung der Aufgabe abgeschlossen oder abgebrochen wurde oder ein Fehler aufgetreten ist
- Die Start- und Endzeit (einschließlich der Gesamtzeit der Übertragung)
- Die Einstellungen der Aufgabe (z. B. Bandbreitenbeschränkungen, Überprüfung der Datenintegrität und andere Optionen für Ihre DataSync Übertragung)

Standardberichte für Aufgaben

Ein Standardaufgabenbericht enthält eine [Zusammenfassung](#) Ihrer Aufgabenausführung sowie detaillierte Berichte darüber, welche DataSync Versuche zu übertragen, zu überspringen, zu überprüfen und zu löschen sind.

Themen

- [Berichtsebene](#)
- [Übertragene Berichte](#)
- [Übersprungene Berichte](#)
- [Verifizierte Berichte](#)
- [Gelöschte Berichte](#)

Berichtsebene

Bei Standardaufgabenberichten können Sie eine der folgenden Berichtsebenen wählen:

- Nur Fehler

- Erfolge und Fehler (im Wesentlichen eine Liste von allem, was während der Ausführung Ihrer Aufgabe passiert ist)

Möglicherweise möchten Sie beispielsweise sehen, welche Dateien während Ihrer Übertragung erfolgreich DataSync übersprungen wurden und welche nicht. Dateien, die erfolgreich DataSync übersprungen wurden, möchten Sie möglicherweise bewusst ausschließen, da sie bereits DataSync an Ihrem Zielort vorhanden sind. Ein übersprungener Fehler kann jedoch beispielsweise darauf hinweisen, dass Sie DataSync nicht über die erforderlichen Berechtigungen zum Lesen einer Datei verfügen.

Übertragene Berichte

Eine Liste von Dateien, Objekten und Verzeichnissen, die während der Ausführung Ihrer Aufgabe DataSync versucht haben, zu übertragen. Ein übertragener Bericht enthält die folgenden Details:

- Die Pfade für die übertragenen Daten
- Was wurde übertragen (Inhalt, Metadaten oder beides)
- Die Metadaten, zu denen der Datentyp, die Inhaltsgröße (nur Objekte und Dateien) und mehr gehören
- Der Zeitpunkt, zu dem ein Element übertragen wurde
- Die Objektversion (wenn das Ziel ein Amazon S3 S3-Bucket ist, für den Versionierung aktiviert ist)
- Wenn im Ziel etwas überschrieben wurde
- Ob ein Artikel erfolgreich übertragen wurde

Note

Wenn Sie Daten zwischen S3-Buckets verschieben, kann das Präfix, das Sie an Ihrem [Quellstandort](#) angeben, in Ihrem Bericht (oder in CloudWatch Amazon-Protokollen) angezeigt werden, auch wenn dieses Präfix nicht als Objekt an Ihrem Zielort existiert. (In der DataSync Konsole stellen Sie möglicherweise auch fest, dass dieses Präfix als übersprungene oder verifizierte Daten angezeigt wird.)

Übersprungene Berichte

Eine Liste von Dateien, Objekten und Verzeichnissen, die in Ihrem Quellverzeichnis DataSync gefunden wurden, aber nicht versucht wurde, sie zu übertragen. Warum Daten DataSync übersprungen werden, kann von verschiedenen Faktoren abhängen, z. B. davon, wie Sie Ihre Aufgabe konfigurieren und welche Speichersystemberechtigungen Sie haben. Hier sind einige Beispiele:

- Es gibt eine Datei, die an Ihren Quell- und Zielorten vorhanden ist. Die Datei in der Quelle wurde seit der letzten Ausführung der Aufgabe nicht geändert. Da Sie [nur Daten übertragen, die sich geändert haben](#), wird diese Datei DataSync nicht übertragen, wenn Sie Ihre Aufgabe das nächste Mal ausführen.
- Ein Objekt, das an beiden Speicherorten vorhanden ist, ändert sich in Ihrer Quelle. Wenn Sie Ihre Aufgabe ausführen, wird dieses Objekt in Ihrem Ziel DataSync übersprungen, da Ihre Aufgabe keine [Daten im Ziel überschreibt](#).
- DataSync überspringt ein Objekt in Ihrer Quelle, das eine [Archivspeicherklasse](#) verwendet und nicht wiederhergestellt wird. Sie müssen ein archiviertes Objekt wiederherstellen, um DataSync es lesen zu können.
- DataSync überspringt eine Datei, ein Objekt oder ein Verzeichnis an Ihrem Quellspeicherort, weil es nicht gelesen werden kann. Wenn dies passiert und nicht zu erwarten ist, überprüfen Sie die Zugriffsberechtigungen Ihres Speichers und stellen Sie sicher, dass gelesen DataSync werden kann, was übersprungen wurde.

Ein übersprungener Bericht enthält die folgenden Details:

- Die Pfade für übersprungene Daten
- Der Zeitpunkt, zu dem ein Element übersprungen wurde
- Der Grund, warum es übersprungen wurde
- Ob ein Artikel erfolgreich übersprungen wurde

Note

Übersprungene Berichte können umfangreich sein, wenn sie Erfolge und Fehler enthalten, Sie Ihre Aufgabe so konfigurieren, [dass nur die Daten übertragen werden, die sich geändert haben](#), und Quelldaten bereits im Ziel vorhanden sind.

Verifizierte Berichte

Eine Liste von Dateien, Objekten und Verzeichnissen, die während der Ausführung Ihrer Aufgabe DataSync versucht haben, deren Integrität zu überprüfen. Ein Bericht mit verifizierten Daten enthält die folgenden Details:

- Die Pfade für verifizierte Daten
- Der Zeitpunkt, zu dem ein Artikel verifiziert wurde
- Der Grund für den Bestätigungsfehler (falls vorhanden)
- Die Quell- und SHA256 Zielprüfsummen (nur Dateien)
- Ob ein Artikel erfolgreich verifiziert wurde

Beachten Sie Folgendes zu verifizierten Berichten:

- Wenn Sie Ihre Aufgabe so konfigurieren, dass [nur übertragene Daten überprüft](#) werden, DataSync werden in manchen Situationen Verzeichnisse oder Dateien oder Objekte, deren Übertragung fehlschlägt, nicht überprüft. In beiden Fällen enthält dieser Bericht DataSync keine unbestätigten Daten.
- Wenn Sie den [erweiterten Modus](#) verwenden, kann die Überprüfung länger als gewöhnlich dauern, wenn Sie große Objekte übertragen.

Gelöschte Berichte

Eine Liste von Dateien, Verzeichnissen und Objekten, die während der Ausführung Ihrer Aufgabe gelöscht wurden. DataSync generiert diesen Bericht nur, wenn Sie [Ihre Aufgabe so konfigurieren](#), dass Daten am Zielort gelöscht werden, die sich nicht in der Quelle befinden. Ein Bericht über gelöschte Daten enthält die folgenden Details:

- Die Pfade für gelöschte Daten
- Ob ein Element erfolgreich gelöscht wurde
- Der Zeitpunkt, zu dem ein Element gelöscht wurde

Beispiele für Aufgabenberichte

Der Detaillierungsgrad Ihres Aufgabenberichts liegt bei Ihnen. Hier sind einige Beispiele für Berichte über übertragene Daten mit der folgenden Konfiguration:

- Berichtstyp — Standard
- Berichtsebene — Erfolge und Fehler

Note

Berichte verwenden den ISO-8601-Standard für das Zeitstempelformat. Die Zeiten sind in UTC angegeben und werden in Nanosekunden gemessen. Dieses Verhalten unterscheidet sich von der Art und Weise, wie einige andere Messwerte für Aufgabenberichte gemessen werden. Beispielsweise werden [Details zur Aufgabenausführung](#), wie `TransferDuration` und `VerifyDuration`, in Millisekunden gemessen.

Aufgabenberichte im erweiterten Modus verwenden ein etwas anderes Schema als Aufgabenberichte im Basismodus. Anhand der folgenden Beispiele können Sie sich ein Bild davon machen, was Sie je nach verwendetem [Aufgabenmodus](#) von Ihren Berichten erwarten können.

Beispiel für übertragene Datenberichte mit Erfolgsstatus

Die folgenden Berichte zeigen erfolgreiche Übertragungen für ein Objekt mit dem Namen `object1.txt`.

Enhanced mode

```
{
  "TaskExecutionId": "exec-abcdefgh12345678",
  "Transferred": [{
    "RelativePath": "object1.txt",
    "SourceMetadata": {
      "Type": "Object",
      "ContentSize": 6,
      "LastModified": "2024-10-04T14:40:55Z",
      "SystemMetadata": {
        "ContentType": "binary/octet-stream",
        "ETag": "\"9b2d7e1f8054c3a2041905d0378e6f14\"",
        "ServerSideEncryption": "AES256"
      },
      "UserMetadata": {},
      "Tags": []
    },
    "Overwrite": "False",
    "DstS3VersionId": "jqtqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
```

```

    "TransferTimestamp": "2024-10-04T14:48:39.748862183Z",
    "TransferType": "CONTENT_AND_METADATA",
    "TransferStatus": "SUCCESS"
  ]
}

```

Basic mode

```

{
  "TaskExecutionId": "exec-abcdefgh12345678",
  "Transferred": [{
    "RelativePath": "/object1.txt",
    "SrcMetadata": {
      "Type": "Regular",
      "ContentSize": 6,
      "Mtime": "2022-01-07T16:59:26.136114671Z",
      "Atime": "2022-01-07T16:59:26.136114671Z",
      "Uid": 0,
      "Gid": 0,
      "Mode": "0644"
    },
    "Overwrite": "False",
    "DstS3VersionId": "jTqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
    "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",
    "TransferType": "CONTENT_AND_METADATA",
    "TransferStatus": "SUCCESS"
  ]
}

```

Beispiel für übertragene Datenberichte mit Fehlerstatus

Die folgenden Berichte enthalten Beispiele dafür, wann ein benanntes Objekt nicht übertragen werden kann. DataSync kann `object1.txt`.

Enhanced mode

Dieser Bericht zeigt, dass `object1.txt` aufgrund eines AWS KMS Berechtigungsproblems nicht auf ein Objekt mit dem Namen zugegriffen werden kann. (Wenn Sie eine solche Fehlermeldung erhalten, finden Sie weitere Informationen unter [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#).)

```

{
  "TaskExecutionId": "exec-abcdefgh12345678",

```

```

"Transferred": [{
  "RelativePath": "object1.txt",
  "SourceMetadata": {
    "Type": "Object",
    "ContentSize": 6,
    "LastModified": "2022-10-07T20:48:32Z",
    "SystemMetadata": {
      "ContentType": "binary/octet-stream",
      "ETag": "\"3a7c0b2f1d9e5c4a6f8b2e0d1c9f7a3b2\"",
      "ServerSideEncryption": "AES256"
    },
    "UserMetadata": {},
    "Tags": []
  },
  "Overwrite": "False",
  "TransferTimestamp": "2022-10-09T16:05:11.134040717Z",
  "TransferType": "CONTENT_AND_METADATA",
  "TransferStatus": "FAILED",
  "ErrorCode": "AccessDenied",
  "ErrorDetail": "User: arn:aws:sts::111222333444:assumed-role/
AWSDataSyncS3Bucket/AwsSync-loc-0b3017fc4ba4a2d8d is not authorized
to perform: kms:GenerateDataKey on resource: arn:aws:kms:us-
east-1:111222333444:key/1111aaaa-22bb-33cc-44d-5555eeee6666 because no identity-
based policy allows the kms:GenerateDataKey action"
}]
}

```

Basic mode

Dieser Bericht zeigt, dass ein Objekt mit dem Namen aufgrund eines S3-Bucket-Berechtigungsproblems `object1.txt` nicht übertragen wurde. (Wenn Sie eine solche Fehlermeldung erhalten, finden Sie weitere Informationen unter [Bereitstellung des DataSync Zugriffs auf S3-Buckets](#).)

```

{
  "TaskExecutionId": "exec-abcdefgh12345678",
  "Transferred": [{
    "RelativePath": "/object1.txt",
    "SrcMetadata": {
      "Type": "Regular",
      "ContentSize": 6,
      "Mtime": "2022-01-07T16:59:26.136114671Z",
      "Atime": "2022-01-07T16:59:26.136114671Z",

```

```
        "Uid": 0,  
        "Gid": 0,  
        "Mode": "0644"  
    },  
    "Overwrite": "False",  
    "DstS3VersionId": "jttqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",  
    "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",  
    "TransferType": "CONTENT_AND_METADATA",  
    "TransferStatus": "FAILED",  
    "FailureReason": "S3 Get Object Failed",  
    "FailureCode": 40974  
  }  
}
```

Einschränkungen

- Einzelne Aufgabenberichte dürfen 5 MB nicht überschreiten. Wenn Sie eine große Anzahl von Dateien kopieren, ist Ihr Aufgabenbericht möglicherweise in mehrere Berichte aufgeteilt.
- Es gibt Situationen, in denen das Erstellen von Aufgabenberichten die Leistung Ihrer Datenübertragung beeinträchtigen kann. Möglicherweise stellen Sie dies fest, wenn Ihre Netzwerkverbindung eine hohe Latenz aufweist und die zu übertragenden Dateien klein sind oder Sie nur Metadatenänderungen kopieren.

Erstellen Sie Ihre DataSync Aufgabenberichte

AWS DataSync Aufgabenberichte können nur eine Zusammenfassung Ihrer Aufgabenausführung oder eine Reihe detaillierter Berichte darüber sein, welche DataSync Versuche zu übertragen, zu überspringen, zu überprüfen und zu löschen sind.

Voraussetzungen

Bevor Sie einen Aufgabenbericht erstellen können, müssen Sie wie folgt vorgehen.

Themen

- [Erstellen Sie einen S3-Bucket für Ihre Aufgabenberichte](#)
- [Erlauben DataSync Sie das Hochladen von Aufgabenberichten in Ihren S3-Bucket](#)

Erstellen Sie einen S3-Bucket für Ihre Aufgabenberichte

Falls Sie noch keinen haben, [erstellen Sie einen S3-Bucket](#), in den Sie Ihren Aufgabenbericht hochladen DataSync können. Berichte werden in der Speicherklasse S3 Standard gespeichert.

Wir empfehlen Folgendes für diesen Bucket:

- Wenn Sie planen, Daten in einen S3-Bucket zu übertragen, verwenden Sie nicht denselben Bucket für Ihren Aufgabenbericht, wenn Sie [die Option Gelöschte Dateien behalten deaktivieren](#). Andernfalls DataSync werden bei jeder Ausführung einer Aufgabe alle vorherigen Aufgabenberichte gelöscht, da diese Berichte an Ihrem Quellspeicherort nicht vorhanden sind.
- Um eine komplexe Einrichtung von Zugriffsberechtigungen zu vermeiden, stellen Sie sicher, dass sich Ihr Aufgabenbericht-Bucket in derselben AWS-Konto Region wie Ihre DataSync Übertragungsaufgabe befindet.

Erlauben DataSync Sie das Hochladen von Aufgabenberichten in Ihren S3-Bucket

Sie müssen eine AWS Identity and Access Management (IAM-) Rolle konfigurieren, die es ermöglicht DataSync , einen Aufgabenbericht in Ihren S3-Bucket hochzuladen.

In der DataSync Konsole können Sie eine IAM-Rolle erstellen, die in den meisten Fällen automatisch die Berechtigungen zum Hochladen eines Aufgabenberichts in Ihren Bucket beinhaltet. Denken Sie daran, dass diese automatisch generierte Rolle unter dem Gesichtspunkt der geringsten Rechte möglicherweise nicht Ihren Anforderungen entspricht. Diese Rolle funktioniert auch nicht, wenn Ihr Bucket mit einem vom Kunden verwalteten AWS Key Management Service (AWS KMS) Schlüssel (SSE-KMS) verschlüsselt ist. In diesen Fällen können Sie die Rolle manuell erstellen, sofern die Rolle mindestens die folgenden Funktionen erfüllt:

- [Beugt dem dienstübergreifenden Problem des verwirrten Stellvertreters](#) in der vertrauenswürdigen Entität der Rolle vor.

Das folgende vollständige Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung verwenden können, um das Problem mit DataSync dem verwirrten Stellvertreter zu verhindern.

JSON

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

```

    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:datasync:us-east-1:123456789012:*"
        }
      }
    }
  ]
}

```

- Ermöglicht DataSync das Hochladen eines Aufgabenberichts in Ihren S3-Bucket.

Das folgende Beispiel tut dies, indem die `s3:PutObject` Aktion nur für ein bestimmtes Präfix (`reports/`) in Ihren Bucket aufgenommen wird.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:PutObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::your-task-reports-bucket/reports/*"
  }]
}

```

- Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten SSE-KMS-Schlüssel verschlüsselt ist, muss die [Richtlinie des Schlüssels](#) die IAM-Rolle enthalten, die für den Zugriff auf den Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#).

Einen nur zusammenfassenden Aufgabenbericht erstellen

Sie können einen Aufgabenbericht konfigurieren, der [nur dann eine Zusammenfassung](#) enthält, wenn Sie Ihre DataSync Aufgabe erstellen, Ihre Aufgabe starten oder Ihre Aufgabe aktualisieren.

Die folgenden Schritte zeigen, wie Sie beim Erstellen einer Aufgabe einen nur zusammenfassenden Aufgabenbericht konfigurieren.

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Scrollen Sie nach unten zum Abschnitt Aufgabenbericht. Wählen Sie als Berichtstyp die Option Nur Zusammenfassung aus.
5. Wählen Sie für S3-Bucket für Berichte einen S3-Bucket aus, in DataSync den Sie Ihren Aufgabenbericht hochladen möchten.

Tip

Wenn Sie planen, Daten in einen S3-Bucket zu übertragen, verwenden Sie nicht denselben Bucket für Ihren Aufgabenbericht, wenn Sie [die Option Gelöschte Dateien behalten deaktivieren](#). Andernfalls DataSync werden bei jeder Ausführung einer Aufgabe alle vorherigen Aufgabenberichte gelöscht, da diese Berichte an Ihrem Quellspeicherort nicht vorhanden sind.

6. Geben Sie unter Ordner ein Präfix ein, das für Ihren Aufgabenbericht verwendet werden soll, wenn der Bericht in Ihren S3-Bucket DataSync hochgeladen wird (z. B. **reports/**).

Achten Sie darauf, das entsprechende Trennzeichen am Ende Ihres Präfixes einzufügen. Dieses Zeichen ist normalerweise ein Schrägstrich (/). / Weitere Informationen finden Sie unter [Objekte mithilfe von Präfixen organisieren](#) im Amazon S3 S3-Benutzerhandbuch.

7. Führen Sie für IAM role (IAM-Rolle) einen der folgenden Schritte aus:

- Wählen Sie Autogenerate, damit DataSync automatisch eine IAM-Rolle mit den Berechtigungen erstellt wird, die für den Zugriff auf den S3-Bucket erforderlich sind.

Wenn Sie DataSync zuvor eine IAM-Rolle für diesen S3-Bucket erstellt haben, wird diese Rolle standardmäßig ausgewählt.

- Wählen Sie eine benutzerdefinierte IAM-Rolle aus, die Sie erstellt haben.

In einigen Fällen müssen Sie die Rolle möglicherweise selbst erstellen. Weitere Informationen finden Sie unter [Erlauben DataSync Sie das Hochladen von Aufgabenberichten in Ihren S3-Bucket](#).

 Important

Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten SSE-KMS-Schlüssel verschlüsselt ist, muss die Richtlinie des Schlüssels die IAM-Rolle enthalten, die für den Zugriff auf den Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#).

8. Beenden Sie die Erstellung Ihrer Aufgabe und [starten Sie dann die Aufgabe, um mit der Übertragung Ihrer Daten zu beginnen](#).

Wenn Ihre Übertragung abgeschlossen ist, können Sie [Ihren Aufgabenbericht einsehen](#).

Mit dem AWS CLI

1. Kopieren Sie den folgenden Befehl create-task AWS Command Line Interface (AWS CLI):

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
  --task-report-config '{
    "Destination":{
      "S3":{
        "Subdirectory":"reports/",
        "S3BucketArn":"arn:aws:s3:::your-task-reports-bucket",
        "BucketAccessRoleArn":"arn:aws:iam::123456789012:role/bucket-iam-role"
```

```
    }
  },
  "OutputType": "SUMMARY_ONLY"
}'
```

2. Geben Sie für den `--source-location-arn` Parameter den Amazon-Ressourcennamen (ARN) des Quellstandorts in Ihrer Übertragung an. `us-east-1` Ersetzen Sie durch die entsprechende Nummer AWS-Region, `123456789012` ersetzen Sie sie durch die entsprechende AWS-Konto Nummer und `12345678abcdefgh` ersetzen Sie sie durch die entsprechende Quellstandort-ID.
3. Geben Sie für den `--destination-location-arn` Parameter den ARN des Zielorts in Ihrer Übertragung an. `us-east-1` Ersetzen Sie durch die entsprechende Nummer AWS-Region, `123456789012` ersetzen Sie sie durch die entsprechende AWS-Konto Nummer und `abcdefgh12345678` ersetzen Sie sie durch die entsprechende Zielstandort-ID.
4. Gehen Sie für den `--task-report-config` Parameter wie folgt vor:
 - Subdirectory— `reports/` Ersetzen Sie es durch das Präfix in Ihrem S3-Bucket, in DataSync den Sie Ihre Aufgabenberichte hochladen möchten.

Achten Sie darauf, das entsprechende Trennzeichen am Ende Ihres Präfixes einzufügen. Dieses Zeichen ist normalerweise ein Schrägstrich (/). Weitere Informationen finden Sie unter [Objekte mithilfe von Präfixen organisieren](#) im Amazon S3 S3-Benutzerhandbuch.

- S3BucketArn— Geben Sie den ARN des S3-Buckets an, in den Sie Ihren Aufgabenbericht hochladen möchten.

Tip

Wenn Sie planen, Daten in einen S3-Bucket zu übertragen, verwenden Sie nicht denselben Bucket für Ihren Aufgabenbericht, wenn Sie [die Option Gelöschte Dateien behalten deaktivieren](#). Andernfalls DataSync werden bei jeder Ausführung einer Aufgabe alle vorherigen Aufgabenberichte gelöscht, da diese Berichte an Ihrem Quellspeicherort nicht vorhanden sind.

- BucketAccessRoleArn— Geben Sie die IAM-Rolle DataSync an, die das Hochladen eines Aufgabenberichts in Ihren S3-Bucket ermöglicht.

Weitere Informationen finden Sie unter [Erlauben DataSync Sie das Hochladen von Aufgabenberichten in Ihren S3-Bucket](#).

⚠ Important

Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten SSE-KMS-Schlüssel verschlüsselt ist, muss die Richtlinie des Schlüssels die IAM-Rolle enthalten, die für den Zugriff auf den Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#).

- `OutputType`— Geben Sie an. `SUMMARY_ONLY`

Weitere Informationen finden Sie unter [Aufgabenberichte nur zusammenfassend](#).

5. Führen Sie den `create-task` Befehl aus, um Ihre Aufgabe zu erstellen.

Sie erhalten eine Antwort wie die folgende, die Ihnen den ARN der Aufgabe zeigt, die Sie erstellt haben. Sie benötigen diesen ARN, um den `start-task-execution` Befehl auszuführen.

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Kopieren Sie den folgenden `start-task-execution` Befehl.

```
aws datasync-task-report start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

7. Geben Sie für den `--task-arn` Parameter den ARN der Aufgabe an, die Sie starten. Verwenden Sie den ARN, den Sie beim Ausführen des `create-task` Befehls erhalten haben.
8. Führen Sie den Befehl `start-task-execution` aus.

Wenn Ihre Übertragung abgeschlossen ist, können Sie [Ihren Aufgabenbericht einsehen](#).

Einen Standard-Aufgabenbericht erstellen

Sie können einen [Standard-Aufgabenbericht](#) konfigurieren, wenn Sie Ihre DataSync Aufgabe erstellen, Ihre Aufgabe starten oder Ihre Aufgabe aktualisieren.

Die folgenden Schritte zeigen, wie Sie beim Erstellen einer Aufgabe einen Standard-Aufgabenbericht konfigurieren.

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Scrollen Sie nach unten zum Abschnitt Aufgabenbericht. Wählen Sie als Berichtstyp die Option Standardbericht aus.
5. Wählen Sie für Berichtsebene eine der folgenden Optionen aus:
 - Nur Fehler — Ihr Aufgabenbericht enthält nur Probleme mit dem, was DataSync übertragen, übersprungen, verifiziert und gelöscht werden sollte.
 - Erfolge und Fehler — Ihr Aufgabenbericht beinhaltet, was DataSync erfolgreich übertragen, übersprungen, verifiziert und gelöscht wurde und was nicht.
 - Benutzerdefiniert — Hier können Sie wählen, ob Sie nur Fehler oder Erfolge und Fehler für bestimmte Aspekte Ihres Aufgabenberichts sehen möchten.

Sie können beispielsweise Erfolge und Fehler für die Liste der übertragenen Dateien auswählen, aber nur Fehler für den Rest des Berichts.

6. Wenn Sie in einen S3-Bucket übertragen, der Objektversionierung verwendet, lassen Sie die Option Amazon S3 S3-Objektversionen einbeziehen aktiviert, wenn Ihr Bericht die neue Version für jedes übertragene Objekt enthalten soll.
7. Wählen Sie für den S3-Bucket für Berichte einen S3-Bucket aus, in den Sie Ihren Aufgabenbericht hochladen DataSync möchten.

Tip

Wenn Sie planen, Daten in einen S3-Bucket zu übertragen, verwenden Sie nicht denselben Bucket für Ihren Aufgabenbericht, wenn Sie [die Option Gelöschte Dateien behalten deaktivieren](#). Andernfalls DataSync werden bei jeder Ausführung einer Aufgabe alle vorherigen Aufgabenberichte gelöscht, da diese Berichte an Ihrem Quellspeicherort nicht vorhanden sind.

8. Geben Sie unter Ordner ein Präfix ein, das für Ihren Aufgabenbericht verwendet werden soll, wenn der Bericht in Ihren S3-Bucket DataSync hochgeladen wird (z. B. **reports/**). Achten Sie darauf, das entsprechende Trennzeichen am Ende Ihres Präfixes einzufügen. Dieses Zeichen ist normalerweise ein Schrägstrich (/). / Weitere Informationen finden Sie unter [Objekte mithilfe von Präfixen organisieren](#) im Amazon S3 S3-Benutzerhandbuch.

9. Führen Sie für IAM role (IAM-Rolle) einen der folgenden Schritte aus:

- Wählen Sie Autogenerate, damit DataSync automatisch eine IAM-Rolle mit den Berechtigungen erstellt wird, die für den Zugriff auf den S3-Bucket erforderlich sind.

Wenn Sie DataSync zuvor eine IAM-Rolle für diesen S3-Bucket erstellt haben, wird diese Rolle standardmäßig ausgewählt.

- Wählen Sie eine benutzerdefinierte IAM-Rolle aus, die Sie erstellt haben.

In einigen Fällen müssen Sie die Rolle möglicherweise selbst erstellen. Weitere Informationen finden Sie unter [Erlauben DataSync Sie das Hochladen von Aufgabenberichten in Ihren S3-Bucket](#).

 Important

Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten SSE-KMS-Schlüssel verschlüsselt ist, muss die Richtlinie des Schlüssels die IAM-Rolle enthalten, die für den Zugriff auf den Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#).

10. Beenden Sie die Erstellung Ihrer Aufgabe und [starten Sie die Aufgabe, um mit der](#) Übertragung Ihrer Daten zu beginnen.

Wenn Ihre Übertragung abgeschlossen ist, können Sie [Ihren Aufgabenbericht einsehen](#).

Mit dem AWS CLI

1. Kopieren Sie den folgenden create-task Befehl:

```
aws datasync create-task \  
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/  
  loc-12345678abcdefgh \
```

```
--destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
--task-report-config '{
  "Destination":{
    "S3":{
      "Subdirectory":"reports/",
      "S3BucketArn":"arn:aws:s3:::your-task-reports-bucket",
      "BucketAccessRoleArn":"arn:aws:iam::123456789012:role/bucket-iam-role"
    }
  },
  "OutputType":"STANDARD",
  "ReportLevel":"level-of-detail",
  "ObjectVersionIds":"include-or-not"
}'
```

2. Geben Sie für den `--source-location-arn` Parameter den ARN des Quellspeicherorts in Ihrer Übertragung an. `us-east-1` Ersetzen Sie durch die entsprechende Nummer AWS-Region, `123456789012` ersetzen Sie sie durch die entsprechende AWS-Konto Nummer und `12345678abcdefgh` ersetzen Sie sie durch die entsprechende Quellstandort-ID.
3. Geben Sie für den `--destination-location-arn` Parameter den ARN des Zielorts in Ihrer Übertragung an. `us-east-1` Ersetzen Sie durch die entsprechende Nummer AWS-Region, `123456789012` ersetzen Sie sie durch die entsprechende AWS-Konto Nummer und `abcdefgh12345678` ersetzen Sie sie durch die entsprechende Zielstandort-ID.
4. Gehen Sie für den `--task-report-config` Parameter wie folgt vor:
 - `Subdirectory`— `reports/` Ersetzen Sie es durch das Präfix in Ihrem S3-Bucket, in DataSync den Sie Ihre Aufgabenberichte hochladen möchten. Achten Sie darauf, das entsprechende Trennzeichen am Ende Ihres Präfixes einzufügen. Dieses Zeichen ist normalerweise ein Schrägstrich (`.`). / Weitere Informationen finden Sie unter [Objekte mithilfe von Präfixen organisieren](#) im Amazon S3 S3-Benutzerhandbuch.
 - `S3BucketArn`— Geben Sie den ARN des S3-Buckets an, in den Sie Ihren Aufgabenbericht hochladen möchten.

 Tip

Wenn Sie planen, Daten in einen S3-Bucket zu übertragen, verwenden Sie nicht denselben Bucket für Ihren Aufgabenbericht, wenn Sie [die Option Gelöschte Dateien behalten deaktivieren](#). Andernfalls DataSync werden bei jeder Ausführung einer

Aufgabe alle vorherigen Aufgabenberichte gelöscht, da diese Berichte an Ihrem Quellspeicherort nicht vorhanden sind.

- `BucketAccessRoleArn`— Geben Sie die IAM-Rolle DataSync an, die das Hochladen eines Aufgabenberichts in Ihren S3-Bucket ermöglicht.

Weitere Informationen finden Sie unter [Erlauben DataSync Sie das Hochladen von Aufgabenberichten in Ihren S3-Bucket](#).

 Important

Wenn Ihr S3-Bucket mit einem vom Kunden verwalteten SSE-KMS-Schlüssel verschlüsselt ist, muss die Richtlinie des Schlüssels die IAM-Rolle enthalten, die für den Zugriff auf den Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#).

- `OutputType`— Geben Sie den Bericht an. STANDARD

Weitere Informationen finden Sie unter [Standardberichte für Aufgaben](#) Typen von Aufgabenberichten.

- (Optional) `ReportLevel` — Geben Sie an, ob Sie `ERRORS_ONLY` dies möchten (Standard) oder `SUCCESSES_AND_ERRORS` in Ihrem Bericht.
- (Optional) `ObjectVersionIds` — Wenn Sie zu einem S3-Bucket wechseln, der Objektversionierung verwendet, geben Sie an, `NONE` ob Sie nicht die neue Version für jedes übertragene Objekt in den Bericht aufnehmen möchten.

Diese Option wird standardmäßig auf `INCLUDE` festgelegt.

- (Optional) `Overrides` — Passen Sie einen bestimmten Aspekt Ihres Berichts an. `ReportLevel`

Vielleicht möchten Sie `SUCCESSES_AND_ERRORS` für die Liste der DataSync gelöschten Dateien an Ihrem Zielort suchen, aber Sie möchten `ERRORS_ONLY` für alles andere. In diesem Beispiel würden Sie dem `--task-report-config` Parameter die folgende `Overrides` Option hinzufügen:

```
"Overrides":{  
  "Deleted":{
```



```
"ReportLevel": "SUCSESSES_AND_ERRORS"
}
```

Wenn Sie es nicht verwenden `Overrides`, verwendet Ihr gesamter Bericht `ReportLevel` das, was Sie angeben.

5. Führen Sie den `create-task` Befehl aus, um Ihre Aufgabe zu erstellen.

Sie erhalten eine Antwort wie die folgende, die Ihnen den ARN der Aufgabe zeigt, die Sie erstellt haben. Sie benötigen diesen ARN, um den `start-task-execution` Befehl auszuführen.

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Kopieren Sie den folgenden `start-task-execution` Befehl.

```
aws datasync-task-report start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

7. Geben Sie für den `--task-arn` Parameter den ARN der Aufgabe an, die Sie gerade ausführen. Verwenden Sie den ARN, den Sie beim Ausführen des `create-task` Befehls erhalten haben.
8. Führen Sie den Befehl `start-task-execution` aus.

Wenn Ihre Übertragung abgeschlossen ist, können Sie [Ihren Aufgabenbericht einsehen](#).

Deine DataSync Aufgabenberichte anzeigen

DataSync erstellt Aufgabenberichte für jede Aufgabenausführung. Wenn Ihre Ausführung abgeschlossen ist, finden Sie die entsprechenden Aufgabenberichte in Ihrem S3-Bucket. Aufgabenberichte sind unter Präfixen organisiert, die IDs Ihrer Aufgaben und deren Ausführung enthalten.

Verwenden Sie diese Beispiele, um Aufgabenberichte in Ihrem S3-Bucket zu finden:

- Aufgabenbericht nur zusammenfassend — *reports-prefix/Summary-Reports/task-id-folder/task-execution-id-folder*
- Standard-Aufgabenbericht — *reports-prefix/Detailed-Reports/task-id-folder/task-execution-id-folder*

Da Aufgabenberichte im JSON-Format vorliegen, haben Sie mehrere Möglichkeiten, Ihre Berichte anzuzeigen:

- Rufen Sie einen Bericht mit [Amazon S3 Select](#) auf.
- Visualisieren Sie Berichte mithilfe von AWS Diensten wie AWS Glue Amazon Athena und Amazon Quick Suite. Weitere Informationen zur Visualisierung Ihrer Aufgabenberichte finden Sie im [AWS Storage-Blog](#).

Überwachung von Datenübertragungen mit Amazon CloudWatch Logs

Sie können Ihre AWS DataSync Übertragung mithilfe von CloudWatch Protokollen überwachen. Wir empfehlen Ihnen, Ihre Aufgabe so zu konfigurieren, dass mindestens grundlegende Informationen (wie Übertragungsfehler) protokolliert werden.

Ermöglicht DataSync das Hochladen von Protokollen in eine CloudWatch Protokollgruppe

Um die [Protokollierung für Ihre DataSync Aufgabe zu konfigurieren](#), benötigen Sie eine CloudWatch Protokollgruppe, DataSync an die Protokolle gesendet werden dürfen. Sie richten diesen Zugriff über eine AWS Identity and Access Management (IAM-) Rolle ein. Wie das konkret funktioniert, hängt von Ihrem [Aufgabenmodus](#) ab.

Enhanced mode

Im erweiterten Modus werden Aufgabenprotokolle DataSync automatisch an eine Protokollgruppe mit dem Namen `aws/datasync` gesendet. Wenn diese Protokollgruppe in Ihrer Region nicht vorhanden ist, erstellt DataSync die Protokollgruppe in Ihrem Namen, indem Sie bei der Erstellung Ihrer Aufgabe eine mit dem [IAM-Dienst verknüpfte Rolle](#) verwenden.

Basic mode

Es gibt mehrere Möglichkeiten, eine CloudWatch Protokollgruppe für eine DataSync Aufgabe im Basismodus einzurichten. In der Konsole können Sie automatisch eine IAM-Rolle erstellen, die in den meisten Fällen die zum Hochladen von Protokollen erforderlichen Berechtigungen umfasst. Beachten Sie, dass diese automatisch generierte Rolle unter dem Gesichtspunkt der geringsten Rechte möglicherweise nicht Ihren Anforderungen entspricht.

Wenn Sie eine vorhandene CloudWatch Protokollgruppe verwenden oder Ihre Aufgaben programmgesteuert erstellen möchten, müssen Sie die IAM-Rolle selbst erstellen.

Das folgende Beispiel ist eine IAM-Richtlinie, die diese Berechtigungen gewährt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncLogsToCloudWatchLogs",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:datasync:us-east-1:444455556666:task/*"
          ]
        },
        "StringEquals": {
          "aws:SourceAccount": "444455556666"
        }
      },
      "Resource": "arn:aws:logs:us-east-1:444455556666:log-group:*:*"
    }
  ]
}
```

Die Richtlinie verwendet Condition Anweisungen, um sicherzustellen, dass nur DataSync Aufgaben aus dem angegebenen Konto Zugriff auf die angegebene CloudWatch Protokollgruppe haben. Es wird empfohlen, in diesen Condition Anweisungen die Kontextschlüssel [aws:SourceArn](#) und die [aws:SourceAccount](#) globale Bedingung zu verwenden, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Weitere Informationen finden Sie unter [Serviceübergreifende Confused-Deputy-Prävention](#).

Um die DataSync Aufgabe oder die Aufgaben zu spezifizieren, *region* ersetzen Sie sie durch den Regionalcode für den AWS-Region Ort, an dem sich die Aufgaben befinden (z. B.us - west -2), und *account-id* ersetzen Sie sie durch die AWS-Konto ID des Kontos, das die Aufgaben enthält. Um die CloudWatch Protokollgruppe anzugeben, ersetzen Sie dieselben Werte. Sie können die Resource Anweisung auch so ändern, dass sie auf bestimmte Protokollgruppen abzielt. Weitere Informationen zur Verwendung von SourceArn und SourceAccount finden Sie unter [Globale Bedingungsschlüssel](#) im IAM-Benutzerhandbuch.

Um die Richtlinie anzuwenden, speichern Sie diese Richtlinienanweisung in einer Datei auf Ihrem lokalen Computer. Führen Sie dann den folgenden AWS CLI Befehl aus, um die Ressourcenrichtlinie anzuwenden. Um diesen Beispielbefehl zu verwenden, *full-path-to-policy-file* ersetzen Sie ihn durch den Pfad zu der Datei, die Ihre Richtlinienanweisung enthält.

```
aws logs put-resource-policy --policy-name trust-datasync --policy-document  
file://full-path-to-policy-file
```

 Note

Führen Sie diesen Befehl aus, indem Sie denselben Befehl verwenden AWS-Konto und den Befehl verwenden AWS-Region , an dem Sie Ihren DataSync Agenten aktiviert haben.

Weitere Informationen finden Sie im [Amazon CloudWatch Logs-Benutzerhandbuch](#).

Konfiguration der Protokollierung für Ihre DataSync Aufgabe

Wir empfehlen, dass Sie mindestens eine gewisse Protokollierungsebene für Ihre DataSync Aufgabe konfigurieren.

Bevor Sie beginnen

DataSync benötigt die Erlaubnis, Protokolle in eine CloudWatch Protokollgruppe hochzuladen. Weitere Informationen finden Sie unter [Ermöglicht DataSync das Hochladen von Protokollen in eine CloudWatch Protokollgruppe](#).

Verwenden der DataSync-Konsole

Die folgenden Anweisungen beschreiben, wie die CloudWatch Protokollierung bei der Erstellung einer Aufgabe konfiguriert wird. Sie können die Protokollierung auch bei der Bearbeitung einer Aufgabe konfigurieren.

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung, wählen Sie dann Aufgaben und anschließend Aufgabe erstellen aus.
3. Konfigurieren Sie die Quell- und Zielorte Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#).

4. Wählen Sie auf der Seite „Einstellungen konfigurieren“ einen [Aufgabenmodus](#) und alle anderen Optionen aus.

Einige der folgenden Optionen könnten Sie interessieren:

- Geben Sie mithilfe eines [Manifests](#) oder von [Filtern](#) an, welche Daten übertragen werden sollen.
 - Konfigurieren Sie, wie [Dateimetadaten behandelt](#) werden sollen, und [überprüfen Sie die Datenintegrität](#).
5. Wählen Sie für Log Level eine der folgenden Optionen aus:
 - Grundinformationen wie Übertragungsfehler protokollieren — Veröffentlichen Sie Protokolle, die nur grundlegende Informationen enthalten (z. B. Übertragungsfehler).
 - Alle übertragenen Objekte und Dateien protokollieren — Veröffentlichen Sie Protokolle für alle Dateien oder Objekte, die DataSync übertragen werden, und führt Datenintegritätsprüfungen durch.
 - Generieren Sie keine Protokolle
 6. Führen Sie je nach Aufgabenmodus, den Sie zum Erstellen oder Angeben einer CloudWatch Protokollgruppe verwenden, einen der folgenden Schritte aus:

Enhanced mode

Wenn Sie Aufgabe erstellen wählen, DataSync wird automatisch eine Protokollgruppe mit dem Namen verwendet (oder erstellt)/aws/datasync.

Basic mode

Geben Sie unter CloudWatch Protokollgruppe eine Protokollgruppe an, die berechtigt DataSync ist, Protokolle hochzuladen, indem Sie einen der folgenden Schritte ausführen:

- Wählen Sie Automatisch generieren, um automatisch eine Protokollgruppe DataSync zu erstellen, in die Protokolle hochgeladen werden können.
- Wählen Sie eine bestehende Protokollgruppe in Ihrer aktuellen AWS-Region Protokollgruppe aus.

Wenn Sie eine bestehende Protokollgruppe auswählen, stellen Sie sicher, dass diese [DataSync Person berechtigt ist](#), Protokolle in diese Protokollgruppe hochzuladen.

7. Wählen Sie Create task aus.

Sie sind bereit, [mit Ihrer Aufgabe zu beginnen](#).

Mit dem AWS CLI

1. Kopieren Sie den folgenden create-task Befehl:

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --task-mode "ENHANCED-or-BASIC" \
  --name "task-name" \
  --options '{"LogLevel": "log-level"}' \
  --cloudwatch-log-group-arn "arn:aws:logs:us-east-1:account-id:log-group:log-group-name:*
```

2. Geben Sie für --source-location-arn den Amazon-Ressourcennamen (ARN) Ihres Quellstandorts an.
3. Geben Sie für --destination-location-arn den ARN Ihres Zielorts an.

Wenn du zwischen AWS-Regionen unseren Konten überweist, vergewissere dich, dass der ARN die andere Region oder Konto-ID enthält.

4. Geben Sie für --task-mode ENHANCED oder anBASIC.

5. (Empfohlen) Geben Sie für `--name` einen Namen für Ihre Aufgabe an, an den Sie sich erinnern können.
6. Geben Sie für `LogLevel` eine der folgenden Optionen an:
 - **BASIC**— Veröffentlichen Sie Protokolle, die nur grundlegende Informationen enthalten (z. B. Übertragungsfehler).
 - **TRANSFER**— Veröffentlichen Sie Protokolle für alle Dateien oder Objekte, die DataSync übertragen und Datenintegritätsprüfungen durchführen.
 - **NONE**— Generieren Sie keine Protokolle.
7. Geben Sie für `--cloudwatch-log-group-arn` den ARN einer CloudWatch Protokollgruppe an.

 Important

Falls `--task-mode` `jaENHANCED`, müssen Sie diese Option nicht angeben. Weitere Informationen finden Sie unter [Ermöglicht DataSync das Hochladen von Protokollen in eine CloudWatch Protokollgruppe](#).

8. Führen Sie den Befehl `create-task` aus.

Wenn der Befehl erfolgreich ist, erhalten Sie eine Antwort, die Ihnen den ARN der Aufgabe anzeigt, die Sie erstellt haben. Beispiel:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Sie sind bereit, [Ihre Aufgabe zu starten](#).

Verwenden der DataSync API

Sie können die CloudWatch Protokollierung für Ihre Aufgabe konfigurieren, indem Sie den `CloudWatchLogGroupArn` Parameter mit einer der folgenden Operationen verwenden:

- [CreateTask](#)
- [UpdateTask](#)

DataSync Task-Protokolle anzeigen

Wenn Sie [Ihre Aufgabe starten](#), können Sie die Protokolle der Aufgabenausführung über die CloudWatch Konsole oder AWS CLI (neben anderen Optionen) einsehen. Weitere Informationen finden Sie im [Amazon CloudWatch Logs-Benutzerhandbuch](#).

DataSync stellt JSON-strukturierte Protokolle für Aufgaben im erweiterten Modus bereit. Aufgaben im Basismodus haben unstrukturierte Protokolle. Die folgenden Beispiele zeigen, wie Überprüfungsfehler in Protokollen im erweiterten Modus im Vergleich zu Protokollen im Basismodus angezeigt werden.

Enhanced mode log example

```
{
  "Action": "VERIFY",
  "Source": {
    "LocationId": "loc-abcdef01234567890",
    "RelativePath": "directory1/directory2/file1.txt"
  },
  "Destination": {
    "LocationId": "loc-05ab2fdc272204a5f",
    "RelativePath": "directory1/directory2/file1.txt",
    "Metadata": {
      "Type": "Object",
      "ContentSize": 66060288,
      "LastModified": "2024-10-03T20:46:58Z",
      "S3": {
        "SystemMetadata": {
          "ContentType": "binary/octet-stream",
          "ETag": "\"1234abcd5678efgh9012ijkl3456mnop\"",
          "ServerSideEncryption": "AES256"
        },
        "UserMetadata": {
          "file-mtime": "1602647222/222919600"
        },
        "Tags": {}
      }
    }
  },
  "ErrorCode": "FileNotAtSource",
  "ErrorDetail": "Verification failed due to file being present at the destination but not at the source"
```



```
}
```

Basic mode log example

```
[NOTICE] Verification failed > /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt  dstMeta: type=R mode=0755 uid=65534
gid=65534 size=8972938 atime=1728657659/0 mtime=1728657659/0 extAttrHash=0
[NOTICE]  dstHash: f9c2cca900301d38b0930367d8d587153154af467da0fdcf1bebc0848ec72c0d
```

AWS DataSync API-Aufrufe protokollieren mit AWS CloudTrail

AWS DataSync ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service Mitglied ausgeführten Aktionen bereitstellt. DataSync CloudTrail erfasst alle API-Aufrufe DataSync als Ereignisse. Zu den aufgezeichneten Aufrufen gehören Aufrufe von der DataSync Konsole und Codeaufrufen für DataSync API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS DataSync. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS DataSync, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Arbeiten mit DataSync Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS DataSync, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS DataSync, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse von allen Ereignissen

AWS-Regionen in derselben AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle DataSync Aktionen werden von protokolliert CloudTrail. (Weitere Informationen finden Sie in der DataSync [API-Referenz](#).)

Beispielsweise generieren Aufrufe der ListLocations Operationen CreateAgentCreateTask, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Anmeldeinformationen gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter [CloudTrail userIdentity Element](#) im AWS CloudTrail Benutzerhandbuch.

DataSync Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, die Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der den CreateTask Vorgang demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::123456789012:user/user1",
    "accountId": "123456789012",
    "accessKeyId": "access key",
    "userName": "user1",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-13T14:56:46Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2018-12-13T14:57:02Z",
  "eventSource": "datasync.amazonaws.com",
  "eventName": "CreateTask",
  "awsRegion": "ap-southeast-1",
  "sourceIPAddress": "192.0.2.1",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "cloudWatchLogGroupArn": "arn:aws:logs:ap-southeast-1:123456789012:log-group:MyLogGroup",
    "name": "MyTask-NTIzMzY1",
    "tags": [],
    "destinationLocationArn": "arn:aws:datasync:ap-southeast-1:123456789012:location/loc-abcdef01234567890",
    "options": {
      "bytesPerSecond": -1,
      "verifyMode": "POINT_IN_TIME_CONSISTENT",
      "uid": "INT_VALUE",
      "posixPermissions": "PRESERVE",
      "mtime": "PRESERVE",
      "gid": "INT_VALUE",
      "preserveDevices": "NONE",
      "preserveDeletedFiles": "REMOVE",
      "atime": "BEST_EFFORT"
    }
  }
}
```

```

    },
    "sourceLocationArn": "arn:aws:datasync:ap-southeast-1:123456789012:location/
loc-021345abcdef6789"
  },
  "responseElements": {
    "taskArn": "arn:aws:datasync:ap-southeast-1:123456789012:task/
task-1234567890abcdef0"
  },
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

Überwachung von Ereignissen mithilfe von Amazon EventBridge

EventBridge Amazon-Ereignisse beschreiben Veränderungen bei DataSync Ressourcen. Sie können Regeln einrichten, die diesen Ereignissen entsprechen und sie an eine oder mehrere Zielfunktionen oder Streams weiterleiten. Ereignisse werden auf die bestmögliche Weise ausgegeben.

DataSync Ereignisse übertragen

Die folgenden EventBridge Ereignisse stehen für DataSync Transfers zur Verfügung.

Agent state changes

Veranstaltung

Status "Online"

Beschreibung

Der Agent ist ordnungsgemäß konfiguriert und einsatzbereit. Dies ist der normale Betriebsstatus für einen Agenten.

Offline

Der Agent hat seit mindestens fünf Minuten keinen Kontakt mehr mit dem DataSync Service aufgenommen. Dies kann verschiedene Gründe haben. Weitere Informationen finden Sie unter [Was mache ich, wenn mein Agent offline ist?](#).

Location state changes

Agent state changes

Veranstaltung	Beschreibung
Hinzufügen	DataSync fügt einen Standort hinzu.
Available (Verfügbar)	Der Speicherort wurde erstellt und ist zur Verwendung verfügbar.

Task state changes

Veranstaltung	Beschreibung
Available (Verfügbar)	Die Aufgabe wurde erstellt und ist startbereit.
In Ausführung	Die Aufgabe ist in Bearbeitung und funktioniert einwandfrei.
Nicht verfügbar	Die Aufgabe ist nicht richtig konfiguriert und kann nicht verwendet werden. Dieses Ereignis wird möglicherweise angezeigt, wenn ein mit der Aufgabe verbundener Agent offline geht.
In Warteschlange eingefügt	Eine andere Aufgabe wird ausgeführt und verwendet denselben Agenten. DataSync führt Aufgaben nacheinander aus (first in, first out).

Task execution state changes

Veranstaltung	Beschreibung
In der Warteschlange	Eine weitere Aufgabenausführung läuft und verwendet denselben DataSync Agenten. Weitere Informationen finden Sie unter Wissen Sie, wann sich Ihre Aufgabe in der Warteschlange befindet.

Agent state changes

Wird gestartet

DataSync initialisiert die Ausführung der Aufgabe. Dieser Status verschwindet normalerweise schnell, kann aber bis zu einigen Minuten dauern.

Schalten Sie die &Snowball;-Appliance ein, indem Sie auf den Ein-/Aus-Schalter über dem E-Ink-Display drücken.

DataSync bestimmt, welche Daten übertragen werden sollen.

Dieser Schritt kann nur wenige Minuten oder einige Stunden dauern, abhängig von der Anzahl der Dateien, Objekte oder Verzeichnisse an beiden Speicherorten und davon, wie Sie Ihre Aufgabe konfigurieren. Die Vorbereitung ist möglicherweise auch nicht auf Ihre Aufgabe anwendbar. Weitere Informationen finden Sie unter [Wie wird Ihre Datenübertragung DataSync vorbereitet.](#)

Übertragung

DataSync führt die eigentliche Datenübertragung durch.

Wird überprüft

DataSync führt am Ende der Übertragung eine Datenintegritätsprüfung durch.

Herzlichen Glückwunsch

Die Ausführung der Aufgabe war erfolgreich.

Abbrechen

Die Ausführung der Aufgabe wird gerade abgebrochen.

Fehler

Die Ausführung der Aufgabe ist fehlgeschlagen.

Überwachung AWS DataSync mit manuellen Tools

Sie können Ihre AWS DataSync Übertragungen von der Konsole oder der Befehlszeile aus verfolgen.

Überwachen Sie Ihre Übertragung mithilfe der DataSync Konsole

Sie können Ihre DataSync Übertragung mithilfe der Konsole überwachen, die Echtzeit-Metriken wie übertragene Daten, Daten- und Dateidurchsatz und Datenkomprimierung bereitstellt.

Um Ihre Übertragung mithilfe der DataSync Konsole zu überwachen

1. Nachdem Sie [Ihre DataSync Aufgabe gestartet](#) haben, wählen Sie Ausführungsdetails anzeigen aus.
2. Sehen Sie sich Kennzahlen zu Ihrer Übertragung an.

Überwachen Sie Ihre Übertragung mithilfe der AWS CLI

Sie können Ihre DataSync Übertragung überwachen, indem Sie AWS Command Line Interface (AWS CLI) verwenden.

Kopieren Sie den folgenden `describe-task-execution` Befehl. Wenn Sie diesen Beispielfehl verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
aws datasync describe-task-execution \
  --task-execution-arn 'arn:aws:datasync:region:account-id:task/task-id/execution/task-
  execution-id'
```

Dieser Befehl gibt Informationen ähnlich wie die folgenden zu einer Aufgabenausführung zurück.

```
{
  "BytesCompressed": 3500,
  "BytesTransferred": 5000,
  "BytesWritten": 5000,
  "EstimatedBytesToTransfer": 5000,
  "EstimatedFilesToDelete": 10,
  "EstimatedFilesToTransfer": 100,
  "FilesDeleted": 10,
  "FilesSkipped": 0,
  "FilesTransferred": 100,
  "FilesVerified": 100,
  "Result": {
    "ErrorCode": "???????",
    "ErrorDetail": "???????",
    "PrepareDuration": 100,
    "PrepareStatus": "SUCCESS",
```

```

        "TransferDuration": 60,
        "TransferStatus": "AVAILABLE",
        "VerifyDuration": 30,
        "VerifyStatus": "SUCCESS"
    },
    "StartTime": 1532660733.39,
    "Status": "SUCCESS",
    "OverrideOptions": {
        "Atime": "BEST_EFFORT",
        "BytesPerSecond": "1000",
        "Gid": "NONE",
        "Mtime": "PRESERVE",
        "PosixPermissions": "PRESERVE",
        "PreserveDevices": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "Uid": "NONE",
        "VerifyMode": "POINT_IN_TIME_CONSISTENT"
    },
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccdddf/execution/exec-1234abcd1234abcd1",
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-datasync-
role",
                "S3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket/*",
                "Subdirectory": "reports"
            }
        },
        "ObjectVersionIds": "INCLUDE",
        "OutputType": "STANDARD",
        "Overrides": {
            "Deleted": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Skipped": {
                "ReportLevel": "SUCCESSSES_AND_ERRORS"
            },
            "Transferred": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Verified": {
                "ReportLevel": "ERRORS_ONLY"
            }
        }
    }
}

```



```
    },  
    "ReportLevel": "ERRORS_ONLY"  
  }  
}
```

- Wenn die Aufgabenausführung erfolgreich ist, ändert sich der Wert von Status zu SUCCESS (ERFOLGREICH). Hinweise zur Bedeutung der Antwortelemente finden Sie unter [DescribeTaskExecution](#).
- Wenn die Ausführung der Aufgabe fehlschlägt, sendet das Ergebnis Fehlercodes, die Ihnen bei der Behebung von Problemen helfen können. Informationen zu den Fehlercodes finden Sie unter [TaskExecutionResultDetail](#).

Überwachen Sie Ihre Übertragung mithilfe des **watch** Dienstprogramms

Um den Fortschritt Ihrer Aufgabe in Echtzeit von der Befehlszeile aus zu überwachen, können Sie das `watch` Unix-Standarddienstprogramm verwenden. Die Werte für die Ausführungsdauer von Aufgaben werden in Millisekunden gemessen.

Das `watch` Hilfsprogramm erkennt den Alias nicht. DataSync Das folgende Beispiel zeigt, wie die CLI direkt aufgerufen wird. Wenn Sie diesen Beispielfehl verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
# pass '-n 1' to update every second and '-d' to highlight differences  
$ watch -n 1 -d \ "aws datasync describe-task-execution --task-execution-arn  
'arn:aws:datasync:region:account-id:task/task-id/execution/task execution-id'"
```

AWS DataSync Ressourcen verwalten

Erfahren Sie, wie Sie Ihre AWS DataSync Ressourcen wie Agenten, Standorte und Aufgaben verwalten.

Ihren DataSync Agenten verwalten

Sobald Sie einen DataSync Agenten aktiviert haben, AWS verwaltet er den Agenten für Sie (einschließlich Softwareupdates). [Weitere Informationen](#)

Testen der Konnektivität und der Systemressourcen Ihres DataSync Agenten

AWS Verwaltet zwar Ihren DataSync Agenten, sobald er bereitgestellt und aktiviert ist, aber es kann vorkommen, dass Sie die Einstellungen Ihres Agenten ändern oder ein Problem beheben müssen.

[Weitere Informationen](#)

Ihren DataSync Agenten ersetzen

Um einen DataSync Agenten zu ersetzen, müssen Sie einen neuen Agenten erstellen und alle Standorte aktualisieren, die den alten Agenten verwenden. [Weitere Informationen](#)

DataSync Ressourcen bereinigen

Wenn Sie Ressourcen DataSync für einen Test verwendet haben oder deren Ressourcen einfach nicht mehr benötigen, löschen Sie diese Ressourcen, damit sie Ihnen nicht in Rechnung gestellt werden. [Weitere Informationen](#)

Die Infrastruktur eines DataSync Agenten wiederverwenden

Nachdem Sie eine Agentenressource von gelöscht haben DataSync, können Sie weiterhin die virtuelle Maschine oder die EC2 Amazon-Instanz des Agenten verwenden, um einen neuen Agenten zu aktivieren. [Weitere Informationen](#)

Ihren AWS DataSync Agenten verwalten

Sobald Sie [einen AWS DataSync Agenten aktiviert](#) haben, AWS verwaltet er die Appliance für virtuelle Maschinen (VM) für Sie.

Softwareupdates für Agenten

AWS aktualisiert automatisch die Software Ihres Agenten, einschließlich des zugrunde liegenden Betriebssystems und der zugehörigen DataSync Softwarepakete.

DataSync aktualisiert Ihren Agenten nur, wenn er inaktiv ist. Beispielsweise wird Ihr Agent erst aktualisiert, wenn Ihre Übertragung abgeschlossen ist.

Der Agent geht nach Aktualisierungen möglicherweise kurzzeitig offline. Dies kann beispielsweise kurz nach der [Aktivierung des Agenten](#) passieren, wenn der Agent AWS aktualisiert wird.

Important

- DataSync Patches werden für Agenten automatisch und regelmäßig aktualisiert, um deren Sicherheit und Stabilität zu gewährleisten. DataSync Agenten im Basismodus verwenden Amazon Linux 2 als Basisbetriebssystem. DataSync Agenten im erweiterten Modus verwenden Amazon Linux 2023 als Basisbetriebssystem. Sie können den aktuellen Status der erkannten Common Vulnerabilities and Exposures (CVE) -Probleme im [Amazon Linux Security Center](#) einsehen. CVE-Patches werden automatisch innerhalb von 30 Tagen nach ihrem Veröffentlichungsdatum installiert, wie im Amazon Linux Security Center angegeben. Das Patchen erfolgt, solange Ihr Agent online ist und keine aktive Aufgabenausführung ausführt.
- DataSync unterstützt nicht die manuelle Aktualisierung eines EC2 Amazon-Agenten mit Cloud-Init-Anweisungen. Wenn Sie einen Agenten auf diese Weise aktualisieren, können Interoperabilitätsprobleme auftreten, DataSync sodass Sie den Agenten nicht aktivieren oder verwenden können.

Status der Agenten

In der folgenden Tabelle wird der Status der DataSync Agenten beschrieben.

Kundendienstmitarbeiter-Status	Bedeutung
Status "Online"	Der Agent ist ordnungsgemäß konfiguriert und einsatzbereit. Dies ist der normale Betriebsstatus für einen Agenten.
Offline	Der Agent hat seit mindestens fünf Minuten keinen Kontakt mehr mit dem DataSync Service aufgenommen. Dies kann verschiedene Gründe haben. Weitere Informationen finden Sie unter Was mache ich, wenn mein Agent offline ist? .

Problembehebung bei Ihrem Agenten

Er AWS verwaltet den DataSync Agenten für Sie, aber es gibt Situationen, in denen Sie möglicherweise erneut direkt mit ihm arbeiten müssen. Wenn Ihr Agent beispielsweise offline geht oder die Verbindung zu Ihrem lokalen Speichersystem verliert, können Sie versuchen, diese Probleme in der [lokalen Konsole des Agenten](#) zu lösen.

Weitere Informationen finden Sie unter [Problembehandlung bei DataSync Agenten](#).

Durchführung von Wartungsarbeiten an Ihrem Agenten

AWS Verwaltet Ihren AWS DataSync Agenten nach der Bereitstellung und Aktivierung, kann es jedoch vorkommen, dass Sie die Einstellungen Ihres Agenten ändern oder ein Problem beheben müssen. Hier sind einige Beispiele dafür, warum Sie mit Ihrem Agenten über dessen lokale Konsole zusammenarbeiten sollten:

- Weisen Sie dem Agenten manuell eine IP-Adresse zu.
- Überprüfen Sie die Systemressourcen Ihres Agenten.

 Important

Für die DataSync Standardfunktionen müssen Sie nicht die lokale Konsole des Agenten verwenden.

Greifen Sie auf die lokale Konsole Ihres Agenten zu

Wie Sie auf die lokale Konsole zugreifen, hängt von der Art des Agenten ab, den Sie verwenden.

Zugreifen auf die lokale Konsole (VMware ESXi, Linux KVM, Nutanix AHV oder Microsoft Hyper-V)

Aus Sicherheitsgründen können Sie keine Remoteverbindung zur lokalen Konsole der virtuellen DataSync Agentenmaschine (VM) herstellen. Sie müssen über Ihre Hypervisor-Verwaltungsschnittstelle auf die lokale Konsole zugreifen.

- Wenn Sie die lokale Konsole zum ersten Mal verwenden, melden Sie sich mit den temporären Anmeldeinformationen an. Der ursprüngliche Benutzername lautet **admin** und das temporäre Passwort lautet **password**. Sie müssen das Passwort bei der ersten Anmeldung ändern.

 Note

Für Agenten im erweiterten Modus gelten die folgenden Kennwortanforderungen:

- Muss mindestens 15 Zeichen enthalten
- Muss mindestens einen Großbuchstaben enthalten
- Muss mindestens einen Kleinbuchstaben enthalten
- Muss mindestens ein numerisches Zeichen enthalten
- Muss mindestens ein Sonderzeichen enthalten
- Mindestens 50% der Zeichen müssen sich bei der Kennwortaktualisierung ändern
- Das Passwort darf kein Wörterbuchwort sein

 Note

Nachdem Sie Ihr Passwort zum ersten Mal eingerichtet haben, können Sie Ihr Passwort jederzeit ändern. Geben Sie im Hauptmenü der Konsole die Zahl neben der

Eingabeaufforderung ein und führen Sie dann den passwd Befehl zum Ändern des Kennworts aus.

Zugreifen auf die lokale Konsole (Amazon EC2)

Um eine Verbindung zur lokalen Konsole eines EC2 Amazon-Agenten herzustellen, müssen Sie SSH verwenden.

Bevor Sie beginnen: Stellen Sie sicher, dass die Sicherheitsgruppe Ihrer EC2 Instance den Zugriff mit SSH (TCP-Port 22) zulässt.

1. Öffnen Sie ein Terminal und kopieren Sie den folgenden ssh Befehl:

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Geben Sie für */path/key-pair-name* den Pfad und den Dateinamen (.pem) des privaten Schlüssels an, der für die Verbindung mit Ihrer Instance erforderlich ist.
 - Legen Sie für *instance-user-name* die Option `admin` fest.
 - Geben Sie für *instance-public-ip-address* die öffentliche IP-Adresse Ihrer Instance an.
2. Führen Sie den ssh Befehl aus, um eine Verbindung mit der Instance herzustellen.

Sobald die Verbindung hergestellt ist, wird das Hauptmenü der lokalen Konsole des Agenten angezeigt.

Konfiguration der DHCP-, DNS- und IP-Einstellungen Ihres Agenten

Die Standardnetzwerkconfiguration für den Agenten ist das Dynamic Host Configuration Protocol (DHCP). Mit dem DHCP wird Ihrem Agent automatisch einer IP-Adresse zugewiesen. In einigen Fällen müssen Sie die IP Ihres Agenten wie im Folgenden beschrieben möglicherweise manuell eine statischen IP-Adresse zuweisen.

1. Melden Sie sich bei der lokalen Konsole Ihres Agenten an.
2. Geben Sie im Hauptmenü AWS DataSync Aktivierung — Konfiguration die Eingabetaste ein, **1** um mit der Konfiguration Ihres Netzwerks zu beginnen.
3. Wählen Sie eine der folgenden Optionen im Menü Network Configuration (Netzwerkconfiguration) aus.

Bis	Vorgehensweise
Abrufen von Informationen zum Netzwerkadapter	Geben Sie 1 ein. Eine Liste mit Adapternamen wird angezeigt, und Sie werden aufgefordert, einen Adapternamen einzugeben, z. B. eth0. Wenn der von Ihnen angegebene Adapter verwendet wird, werden Netzwerkinformationen für diesen Adapter angezeigt, wie im folgenden Beispiel: <pre>IP Preference: IPv4 MAC address: 52:54:12:a4:f7:7d IPv4 address: 192.168.100.482 Netmask: 255.255.255.0 Gateway: 192.168.100.4 DHCP enabled: Yes IPv6 address: abcd:4444:e5ee:fd00::4daf Prefix length: 128 Gateway: fe80::5021:ff:ff88:4acd DHCPV6 enabled: Yes DNS: abcd:4444:e5ee:fd00::1 DNS: 192.168.100.4</pre> Sie verwenden denselben Adaptername für die Konfiguration einer statischen IP-Adresse (Option 3) wie für die Einrichtung des Standard-Route-Adapters Ihres Agenten (Option 5).

Bis	Vorgehensweise
Konfigurieren von DHCP	Geben Sie 2 ein. Wählen Sie eine zu verwendende IP-Version aus, und konfigurieren Sie dann die Netzwerkschnittstelle für die Verwendung von DHCP.
Konfigurieren einer statischen IP-Adresse für Ihren Agenten	Geben Sie 3 ein. Sie werden aufgefordert, das zu verwendende IP-Protokoll, IPv4 IPv6, oder beides auszuwählen. Anschließend werden Sie aufgefordert, den Namen des Netzwerkadapters einzugeben, um eine statische IP-Adresse zu konfigurieren.  Important Wenn Ihr Agent bereits aktiviert wurde, müssen Sie ihn herunterfahren und von der DataSync Konsole aus neu starten, damit die Einstellungen wirksam werden.

Bis	Vorgehensweise
Zurücksetzen der Netzwerkkonfiguration Ihres Agenten auf DHCP	Geben Sie 4 ein. Wählen Sie die IP-Version aus, die auf DHCP zurückgesetzt werden soll. Alle Netzwerkschnittstellen für die gewählte IP-Version sind so eingestellt, dass sie DHCP verwenden.  Important Wenn Ihr Agent bereits aktiviert wurde, müssen Sie Ihren Agenten von der DataSync Konsole aus herunterfahren und neu starten, damit die Einstellungen wirksam werden.
Einrichten des Standard-Routing-Adapters Ihres Agenten	Geben Sie 5 ein. Die verfügbaren Adapter für Ihren Agenten werden angezeigt, und Sie werden aufgefordert, einen der Adapter auszuwählen, z. B. eth0
Bearbeiten Sie die DNS-Konfiguration (Domain Name System) Ihres Agenten	Geben Sie 6 ein. Die verfügbaren Adapter des primären und sekundären DNS-Servers werden angezeigt. Sie werden aufgefordert, die neue IP-Adresse einzugeben.

Bis	Vorgehensweise
Anzeigen der DNS-Konfiguration Ihres Agenten	Geben Sie 7 ein. Die verfügbaren Adapter des primären und sekundären DNS-Servers werden angezeigt.  Note Bei einigen Versionen des VMware Hypervisors können Sie die Adapterkonfiguration in diesem Menü bearbeiten.
Anzeigen von Routing-Tabellen	Geben Sie 8 ein. Wählen Sie die IP-Version (IPv4 IPv6, oder beide), um die Standard-Routing-Tabelle für Ihren Agenten anzuzeigen.
Zeigen Sie die IP-Version Ihres Agenten für Datenübertragungen an	Geben Sie 9 ein. Die IP-Versionseinstellung des Agenten für Datenübertragungen wird entweder IPv4, IPv6IPv4 (auto), oder angezeigtIPv6 (auto).

Bis	Vorgehensweise
Bearbeiten Sie das IP-Protokoll Ihres Agenten für Datenübertragungen	Geben Sie 10 ein. Die verfügbaren IP-Versionseinstellungen für Datenübertragungen werden angezeigt. Sie können entweder IPv4, IPv6IPv4 (auto), oder wählen IPv6 (auto). Weitere Informationen zu den IP-Versionseinstellungen Ihres Agenten für Datenübertragungen finden Sie unter the section called “IPv6 Unterstützung”.

Überprüfen Sie die Systemressourcen Ihres Agenten

Wenn Sie sich an Ihrer Agentenkonsole anmelden, werden die virtuellen CPU-Kerne, die Größe des Root-Volumes und der Arbeitsspeicher automatisch überprüft. Wenn Fehler oder Warnungen vorliegen, werden diese im Konsolenmenü mit einem Banner gekennzeichnet, das Einzelheiten zu diesen Fehlern oder Warnungen enthält.

Wenn beim Start der Konsole keine Fehler oder Warnungen angezeigt werden, wird im Menü weißer Text angezeigt. Die Option Systemressourcenprüfung anzeigen wird angezeigt (0 Errors).

Wenn Fehler oder Warnungen vorliegen, zeigt das Konsolenmenü die Anzahl der Fehler und Warnungen in Rot bzw. Gelb in einem Banner oben im Menü an. Beispiel, (1 ERROR, 1 WARNING).

Um die Systemressourcen Ihres Agenten zu überprüfen

1. Melden Sie sich bei der lokalen Konsole Ihres Agenten an.
2. Geben Sie im Hauptmenü AWS DataSync Aktivierung — Konfiguration die Eingabetaste ein, **4** um die Ergebnisse der Systemressourcenprüfung einzusehen.

Die Konsole zeigt für jede Ressource [OK], [WARNING] ([WARNUNG]) oder [FAIL] ([FEHLGESCHLAGEN]) an (siehe folgende Tabelle).

Bei EC2 Amazon-Instances überprüft die Systemressourcenprüfung, ob es sich bei dem Instance-Typ um einen der für die Verwendung empfohlenen Instances handelt. DataSync Wenn

der Instance-Typ mit dieser Liste übereinstimmt, wird ein einzelnes Ergebnis wie folgt in grünem Text angezeigt.

[OK] Instance Type Check

Wenn die EC2 Amazon-Instance nicht auf der empfohlenen Liste steht, werden bei der Systemressourcenprüfung die folgenden Ressourcen überprüft.

- Prüfung der CPU-Kerne: Es sind mindestens vier Kerne erforderlich.
- Überprüfung der Festplattengröße: Es sind mindestens 80 GB verfügbarer Festplattenspeicher erforderlich.
- RAM-Prüfung:
 - 32 GB RAM wurden der Instanz für Aufgabenausführungen zugewiesen, die mit bis zu 20 Millionen Dateien, Objekten oder Verzeichnissen arbeiten.
 - 64 GB RAM wurden der Instanz für Aufgabenausführungen zugewiesen, die mit mehr als 20 Millionen Dateien, Objekten oder Verzeichnissen arbeiten.
- Überprüfung der CPU-Flags: Die Agent-VM-CPU muss entweder über Befehlssatz-Flags SSSE3 oder über SSE4 Befehlssatzflags verfügen.

Wenn die EC2 Amazon-Instance nicht auf der Liste der empfohlenen Instances für steht DataSync, aber über ausreichende Ressourcen verfügt, zeigt das Ergebnis der Systemressourcenprüfung vier Ergebnisse an, alle in grünem Text.

Dieselben Ressourcen wurden für Agenten verifiziert, die in Hyper-V, Linux Kernel-based Virtual Machine (KVM) und bereitgestellt werden. VMware VMs

VMware Agenten werden auch auf unterstützte Versionen überprüft. Nicht unterstützte Versionen führen zu einem roten Banner-Fehler. Zu den unterstützten Versionen gehören die VMware Versionen 6.5 und 6.7.

Serverkonfiguration für die Systemzeit des Agenten anzeigen und verwalten

Sie können die Systemzeit-Serverkonfiguration Ihres Agenten anzeigen und verwalten.

1. Melden Sie sich bei der [lokalen Konsole](#) Ihres Agenten an.
2. Geben Sie im Hauptmenü AWS DataSync Aktivierung — Konfiguration die Option für die Systemzeitverwaltung (z. B. 5 für den VMware Agenten) ein.

3. Führen Sie im Menü System Time Management einen der folgenden Schritte aus:

Bis	Vorgehensweise
Systemzeit und Dienststatus anzeigen	Geben Sie 1 ein. Zeigen Sie die aktuelle Systemzeit in UTC, den Zeitdienststatus, die aktiven Zeitserver und den Synchronisierungsstatus an.
Synchronisieren Sie die Systemzeit	Geben Sie 2 ein. Es wird eine Aufforderung angezeigt, den Zeitserver sofort zu synchronisieren. In einigen Situationen kann es vorkommen , dass die Zeit eines Agenten schwankt. Beispielsweise kann es zu einem längeren Netzwerkausfall kommen und Ihr Hypervisor-Host und -Agent erhalten keine Zeitaktualisierungen, sodass die Uhrzeit Ihres Agenten von der tatsächlichen Zeit abweicht. Bei einer solchen Zeitabweichung kommt es zu einer Diskrepanz zwischen den angegebenen Zeiten, zu denen Vorgänge (z. B. Snapshots) ausgeführt werden, und den tatsächlichen Zeiten, zu denen die Vorgänge ausgeführt werden.
Starten Sie den Systemzeitdienst neu	Geben Sie 3 ein. Es wird eine Aufforderung angezeigt, den Zeitsynchronisierungsdienst neu zu starten.

Bis	Vorgehensweise
Die Konfiguration des Zeitservers verwalten	Geben Sie 4 ein. Zeigen Sie Ihre Zeitserver-Einstellungen an und verwalten Sie sie. Fügen Sie Zeitserver und Serverpools hinzu oder entfernen Sie sie und legen Sie bevorzugte Server für eine präzise Synchronisation fest.

Befehle im Zusammenhang mit der Wartung für Ihren Agenten ausführen

In der lokalen Konsole Ihres DataSync Agenten können Sie einige Wartungsaufgaben ausführen und Probleme mit Ihrem Agenten diagnostizieren.

Um einen Konfigurations- oder Diagnosebefehl in der lokalen Konsole Ihres Agenten auszuführen

1. Melden Sie sich bei [der lokalen Konsole Ihres Agenten](#) an.
2. Geben Sie im Hauptmenü AWS DataSync Aktivierung — Konfiguration in der Befehlszeile **5** (oder **6** für eine VMware VM) ein.
3. Verwenden Sie die folgenden Befehle, um die folgenden Aufgaben mit Ihrem Agenten auszuführen.

Befehl	Description
dig	Suchen Sie nach DNS-Informationen über den Host.
diskclean	Führen Sie eine Festplattenbereinigung durch.
exit	Kehren Sie zum Konfigurationsmenü der Konsole zurück.
h	Zeigt eine Liste der verfügbaren Befehle an.
ifconfig	Netzwerkschnittstellen anzeigen oder konfigurieren.

Befehl	Description
ip	Routing, Geräte und Tunnel anzeigen oder konfigurieren.
iptables	IPv4 Paketfilterung und NAT einrichten und verwalten.
ip6tables	IPv6 Paketfilterung und NAT einrichten und verwalten.
ncport	Testen Sie die Konnektivität zu einem bestimmten Netzwerk-TCP-Port.
nping	Hier finden Sie Informationen zur Behebung von Netzwerkproblemen.
passwd	Benutzerpasswort ändern.
save-iptables	Speichern Sie die Firewallregeln für IPv4 Tabellen dauerhaft.
save-ip6tables	Speichern Sie die Firewallregeln für IPv6 Tabellen dauerhaft.
save-routing-table	Speichern Sie einen neu hinzugefügten Routing-Tabelleneintrag.
sslcheck	Überprüfen Sie, ob ein SSL-Zertifikat gültig ist.
tcptraceroute	Erfassen Sie die <code>traceroute</code> Ausgabe des TCP-Datenverkehrs zu einem Ziel.

4. Folgen Sie den Anweisungen auf dem Bildschirm.

Ihren AWS DataSync Agenten ersetzen

Um einen AWS DataSync Agenten zu ersetzen, müssen Sie einen neuen Agenten erstellen und alle Übertragungsorte aktualisieren, die den alten Agenten verwenden.

Einen neuen Agenten erstellen

Um Ihren neuen DataSync Agenten zu erstellen, gehen Sie genauso vor, wie Sie Ihren alten Agenten erstellt haben:

1. [Stellen Sie einen Agenten](#) in Ihrer Speicherumgebung bereit.
2. [Wählen Sie einen Service-Endpunkt](#), mit dem der Agent kommuniziert AWS.
3. [Konfigurieren Sie Ihr Netzwerk](#) so, dass der Agent mit Ihrem Speicher kommunizieren kann und AWS.
4. [Aktivieren Sie Ihren Agenten](#).
5. Notieren Sie sich nach der Aktivierung den Amazon-Ressourcennamen (ARN) des Agenten.

Sie benötigen diesen ARN, wenn Sie Ihren DataSync Standort aktualisieren, um den neuen Agenten verwenden zu können.

Aktualisierung Ihres Standorts mit dem neuen Agenten

Sobald Sie einen neuen Agenten erstellt haben, können Sie einen vorhandenen DataSync Standort aktualisieren, um diesen Agenten zu verwenden. In den meisten Fällen müssen Sie auch die Zugangsdaten erneut eingeben, um den Standort zu aktualisieren. Dies liegt daran, dass die Anmeldeinformationen für den Standort so DataSync gespeichert werden, dass nur Ihr Agent sie verwenden kann.

Verwenden der DataSync Konsole

In den folgenden Anweisungen wird beschrieben, wie Sie Standorte mithilfe der DataSync Konsole mit einem neuen Agenten aktualisieren.

NFS

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
3. Wählen Sie den Standort aus, den Sie aktualisieren möchten, und klicken Sie dann auf Bearbeiten.
4. Wählen Sie für Agenten Ihren neuen Agenten aus.

Sie können mehr als einen Agenten auswählen, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen möchten.

5. Wählen Sie Änderungen speichern.

SMB

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
3. Wählen Sie den Standort aus, den Sie aktualisieren möchten, und klicken Sie dann auf Bearbeiten.
4. Wählen Sie für Agenten Ihren neuen Agenten aus.

Sie können mehr als einen Agenten auswählen, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen möchten.

5. Geben Sie unter Passwort das Passwort des Benutzers ein, der Ihren SMB-Dateiserver bereitstellen kann und über Zugriffsrechte auf die Dateien und Ordner verfügt, die an Ihrer Übertragung beteiligt sind.
6. Wählen Sie Änderungen speichern.

HDFS

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
3. Wählen Sie den Standort aus, den Sie aktualisieren möchten, und klicken Sie dann auf Bearbeiten.
4. Wählen Sie für Agenten Ihren neuen Agenten aus.

Sie können mehr als einen Agenten auswählen, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen möchten.

5. Wenn Sie die Kerberos-Authentifizierung verwenden, laden Sie Ihre Keytab-Datei und die Kerberos-Konfigurationsdatei hoch.
6. Wählen Sie Änderungen speichern.

Object storage

1. Öffnen Sie die Konsole unter. AWS DataSync <https://console.aws.amazon.com/datasync/>
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
3. Wählen Sie den Standort aus, den Sie aktualisieren möchten, und klicken Sie dann auf Bearbeiten.
4. Wählen Sie für Agenten Ihren neuen Agenten aus.

Sie können mehr als einen Agenten auswählen, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen möchten.

5. Wenn für Ihren Standort Anmeldeinformationen erforderlich sind, geben Sie den geheimen Schlüssel ein, der den DataSync Zugriff auf Ihren Objektspeicher-Bucket ermöglicht.
6. Wählen Sie Änderungen speichern.

Azure Blob Storage

Gehen Sie wie folgt vor, um Ihre zu aktualisieren Microsoft Azure Blob Storage Standort:

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
3. Wählen Sie den Standort aus, den Sie aktualisieren möchten, und klicken Sie dann auf Bearbeiten.
4. Wählen Sie für Agenten Ihren neuen Agenten aus.

Sie können mehr als einen Agenten auswählen, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen möchten.

5. Geben Sie als SAS-Token das [Shared Access Signature \(SAS\) -Token](#) ein, das DataSync den Zugriff auf Ihren Blob-Speicher ermöglicht.
6. Wählen Sie Änderungen speichern.

Verwenden Sie den AWS CLI

Die folgenden Anweisungen beschreiben, wie Sie Standorte mit einem neuen Agenten aktualisieren, indem Sie den verwenden AWS CLI. (Sie können dies auch mithilfe der [DataSync API](#) tun.)

NFS

1. Kopieren Sie den folgenden [update-location-nfs](#) Befehl:

```
aws datasync update-location-nfs \  
  --location-arn datasync-nfs-location-arn \  
  --on-prem-config AgentArns=new-datasync-agent-arn
```

2. Geben Sie für den `--location-arn` Parameter den ARN des NFS-Speicherorts an, den Sie aktualisieren.
3. Geben Sie für die `AgentArns` Option des `--on-prem-config` Parameters den ARN Ihres neuen Agenten an.

Sie können mehr als einen ARN angeben, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen.

4. Führen Sie den `update-location-nfs` Befehl aus, um den Standort zu aktualisieren.

SMB

1. Kopieren Sie den folgenden [update-location-smb](#) Befehl:

```
aws datasync update-location-smb \  
  --location-arn datasync-smb-location-arn \  
  --agent-arns new-datasync-agent-arn \  
  --password smb-file-server-password
```

2. Geben Sie für den `--location-arn` Parameter den ARN des SMB-Standorts an, den Sie aktualisieren.
3. Geben Sie für den `--agent-arns` Parameter den ARN Ihres neuen Agenten an.

Sie können mehr als einen ARN angeben, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen.

4. Geben Sie für den `--password` Parameter das Passwort des Benutzers an, der Ihren SMB-Dateiserver bereitstellen kann und berechtigt ist, auf die Dateien und Ordner zuzugreifen, die an Ihrer Übertragung beteiligt sind.
5. Führen Sie den `update-location-smb` Befehl aus, um den Speicherort zu aktualisieren.

HDFS

1. Kopieren Sie den folgenden `update-location-hdfs` Befehl:

```
aws datasync update-location-hdfts \
  --location-arn datasync-hdfts-location-arn \
  --agent-arns new-datasync-agent-arn \
  --kerberos-keytab keytab-file \
  --kerberos-krb5-conf krb5-conf-file
```

2. Geben Sie für den `--location-arn` Parameter den ARN des HDFS-Speicherorts an, den Sie aktualisieren.
3. Geben Sie für den `--agent-arns` Parameter den ARN Ihres neuen Agenten an.

Sie können mehr als einen ARN angeben, wenn Sie mehrere Agenten für einen Standort ersetzen.

4. Wenn Sie die Kerberos-Authentifizierung verwenden, geben Sie die Parameter `--kerberos-keytab` und `--kerberos-krb5-conf` an:

- Geben Sie für den `--kerberos-keytab` Parameter die Kerberos-Schlüsseltabelle (Keytab) an, die Zuordnungen zwischen dem definierten Kerberos-Prinzipal und den verschlüsselten Schlüsseln enthält.

Sie können die Keytab-Datei angeben, indem Sie die Adresse der Datei angeben.

- Geben Sie für den `--kerberos-krb5-conf` Parameter die Datei an, die die Konfiguration für Ihren Kerberos-Bereich enthält.

Sie können die `krb5.conf` Datei angeben, indem Sie die Adresse der Datei angeben.

Wenn Sie die einfache Authentifizierung verwenden, müssen Sie diese Kerberos-bezogenen Parameter nicht in Ihren Befehl aufnehmen.

5. Führen Sie den `update-location-hdfs` Befehl aus, um den Speicherort zu aktualisieren.

Object storage

1. Kopieren Sie den folgenden `update-location-object-storage` Befehl:

```
aws datasync update-location-object-storage \
```

```
--location-arn datasync-object-storage-location-arn \  
--agent-arns new-datasync-agent-arn \  
--secret-key bucket-secret-key
```

2. Geben Sie für den `--location-arn` Parameter den ARN des Objektspeichers an, den Sie aktualisieren.
3. Geben Sie für den `--agent-arns` Parameter den ARN Ihres neuen Agenten an.

Sie können mehr als einen ARN angeben, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen.

4. Gehen Sie wie folgt vor, je nachdem, ob Ihr Objektspeicherort Zugangsdaten erfordert:
 - Wenn für Ihren Standort Anmeldeinformationen erforderlich sind — Geben Sie für den `--secret-key` Parameter den geheimen Schlüssel an, der den DataSync Zugriff auf Ihren Objektspeicher-Bucket ermöglicht.
 - Wenn für Ihren Standort Anmeldeinformationen erforderlich sind — Geben Sie leere Zeichenfolgen für die `--secret-key` Parameter `--access-key` und an. Hier ist ein Beispielbefehl:

```
aws datasync update-location-object-storage \  
  --location-arn arn:aws:datasync:us-east-2:111122223333:location/  
  loc-abcdef01234567890 \  
  --agent-arns arn:aws:datasync:us-east-2:111122223333:agent/  
  agent-1234567890abcdef0 \  
  --access-key "" \  
  --secret-key ""
```

5. Führen Sie den `update-location-object-storage` Befehl aus, um den Standort zu aktualisieren.

Azure Blob Storage

1. Kopieren Sie den folgenden [update-location-azure-blob](#) Befehl:

```
aws datasync update-location-azure-blob \  
  --location-arn datasync-azure-blob-storage-location-arn \  
  --agent-arns new-datasync-agent-arn \  
  --sas-configuration '{  
    "Token": "sas-token-for-azure-blob-storage"
```

```
}'
```

2. Geben Sie für den `--location-arn` Parameter den ARN des Azure Blob Storage Standort, den Sie aktualisieren.
3. Geben Sie für den `--agent-arns` Parameter den ARN Ihres neuen Agenten an.

Sie können mehr als einen ARN angeben, wenn Sie [mehrere Agenten](#) für einen Standort ersetzen.

4. Geben Sie für die Token Option des `--sas-configuration` Parameters das [SAS-Token](#) an, das den DataSync Zugriff auf Ihren Blob-Speicher ermöglicht.
5. Führen Sie den `update-location-azure-blob` Befehl aus, um den Speicherort zu aktualisieren.

Nächste Schritte

1. [Löschen Sie Ihren alten Agenten](#). Wenn Sie DataSync Aufgaben ausführen, die diesen Agenten verwenden, warten Sie, bis diese Aufgaben abgeschlossen sind, bevor Sie ihn löschen.
2. Wenn Sie Agenten für mehrere Standorte ersetzen müssen, wiederholen Sie die vorherigen Schritte.
3. Wenn Sie fertig sind, können Sie [Ihre Aufgaben wieder ausführen](#).

Note

Agenten für geplante Aufgaben ersetzen — Wenn Sie einen Agenten für eine [geplante Aufgabe](#) ersetzen, müssen Sie diese Aufgabe manuell starten, wenn der neue Agent einen anderen Typ von [Service-Endpunkt](#) verwendet als Ihr alter Agent. Wenn Sie die Aufgabe vor der nächsten geplanten Ausführung nicht manuell ausführen, schlägt die Aufgabe fehl.

Wenn Ihr alter Agent beispielsweise einen öffentlichen Dienstendpunkt verwendet hat, der neue Agent jedoch einen VPC-Endpunkt verwendet, starten Sie diese Aufgabe manuell über die Konsole oder den `StartTaskExecution` Vorgang. Danach wird Ihre Aufgabe wieder wie geplant ausgeführt.

AWS DataSync Ressourcen filtern

Sie können Ihre AWS DataSync Standorte und Aufgaben filtern, indem Sie die `ListTasks` API-Operationen `ListLocations` und in der verwenden AWS CLI. Rufen Sie beispielsweise eine Liste Ihrer letzten Aufgaben ab.

Parameter für die Filterung

Sie können API-Filter verwenden, um die Liste der von `ListTasks` und zurückgegebenen Ressourcen einzugrenzen `ListLocations`. Um beispielsweise alle Ihre Amazon S3 S3-Standorte abzurufen, können Sie `ListLocations` mit dem Filternamen `LocationType S3` und verwenden Operator `Equals`.

Um API-Ergebnisse zu filtern, müssen Sie einen Filternamen, einen Operator und einen Wert angeben.

- **Name**— Der Name des Filters, der verwendet wird. Jeder API-Aufruf unterstützt eine Liste von Filtern, die für ihn verfügbar sind (z. B. `LocationType` für `ListLocations`).
- **Values**— Die Werte, nach denen Sie filtern möchten. Beispielsweise möchten Sie möglicherweise nur Amazon S3 S3-Standorte anzeigen.
- **Operator**— Der Operator, der zum Vergleichen von Filterwerten verwendet wird (z. B. `Equals` oder `Contains`).

In der folgenden Tabelle sind die verfügbaren Operatoren aufgeführt.

Operator	Schlüsseltypen
<code>Equals</code>	Zeichenfolge, Zahl
<code>NotEquals</code>	Zeichenfolge, Zahl
<code>LessThan</code>	Zahl
<code>LessThanOrEqualTo</code>	Zahl
<code>GreaterThan</code>	Zahl
<code>GreaterThanOrEqualTo</code>	Zahl

Operator	Schlüsseltypen
In	Zeichenfolge
Contains	Zeichenfolge
NotContains	Zeichenfolge
BeginsWith	Zeichenfolge

Nach Standort filtern

ListLocations unterstützt die folgenden Filternamen:

- **LocationType**— Filtert nach dem Standorttyp:
 - SMB
 - NFS
 - HDFS
 - OBJECT_STORAGE
 - S3
 - OUTPOST_S3
 - FSX_WINDOWS
 - FSX_LUSTRE
 - FSX_OPENZFS_NFS
 - FSX_ONTAP_NFS
 - FSX_ONTAP_SMB
- **LocationUri**— Filtert nach dem Uniform Resource Identifier (URI), der dem Standort zugewiesen wurde, wie er vom DescribeLocation* API-Aufruf zurückgegeben wurde (z. B. `s3://bucket-name/your-prefix` für Amazon S3 S3-Standorte).
- **CreationTime**— Filtert nach dem Zeitpunkt, zu dem der Standort erstellt wurde. Das Eingabeformat ist `yyyy-MM-dd:mm:ss` in koordinierter Weltzeit (UTC) angegeben.

Das folgende AWS CLI Beispiel listet alle Standorte des Typs Amazon S3 auf, deren Standort-URI mit der Zeichenfolge beginnt "s3://amzn-s3-demo-bucket" und die am 15.12.2019 um 17:15:20 UTC oder danach erstellt wurden.

```
aws datasync list-locations \
  --filters [{Name=LocationType, Values=["S3"], Operator=Equals},
  {Name=LocationUri, Values=["s3://amzn-s3-demo-bucket"], Operator=BeginsWith},
  {Name=CreationTime, Values=["2019-12-15 17:15:20"], Operator=GreaterThanOrEqualTo}]
```

Dieser Befehl gibt etwa die folgende Ausgabe zurück.

```
{
  "Locations": [
    {
      "LocationArn": "arn:aws:datasync:us-east-1:111122223333:location/loc-3333333333abcdef0",
      "LocationUri": "s3://amzn-s3-demo-bucket1/"
    },
    {
      "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/loc-987654321abcdef0",
      "LocationUri": "s3://amzn-s3-demo-bucket2/"
    }
  ]
}
```

Nach Aufgabe filtern

ListTasks unterstützt die folgenden Filternamen.

- **LocationId**— Filtert sowohl nach Quell- als auch nach Zielorten nach Werten für Amazon Resource Name (ARN).
- **CreationTime**— Filtert nach dem Zeitpunkt, zu dem die Aufgabe erstellt wurde. Das Eingabeformat ist yyyy-MM-dd:mm:ss in UTC.

Das folgende AWS CLI Beispiel zeigt die Syntax beim Filtern nach LocationId.

```
aws datasync list-tasks \
  --filters Name=LocationId,Values=arn:aws:datasync:us-east-1:your-account-id:location/your-location-id,Operator=Contains
```

Die Ausgabe dieses Befehls sieht in etwa wie folgt aus.

```
{
  "Tasks": [
    {
      "TaskArn": "arn:aws:datasync:us-east-1:your-account-id:task/your-task-id",
      "Status": "AVAILABLE",
      "Name": "amzn-s3-demo-bucket"
    }
  ]
}
```

Bereinigen Sie Ihre AWS DataSync Ressourcen

Wenn Sie die von Ihnen erstellten AWS Ressourcen AWS DataSync für einen Test verwendet haben oder nicht benötigen, löschen Sie sie, damit Ihnen keine Ressourcen in Rechnung gestellt werden, die Sie nicht nutzen möchten.

Note

Wenn Sie DataSync Ressourcen in einer [Opt-in-Region](#) haben, die Sie deaktivieren, werden diese Ressourcen nicht automatisch gelöscht. Die Ressourcen sind weiterhin vorhanden, wenn Sie diese Region erneut aktivieren.

Einen DataSync Agenten löschen

Wenn Sie einen Agenten von löschen AWS DataSync, ist die Agentenressource nicht mehr mit Ihrem verknüpft AWS-Konto und kann auch nicht rückgängig gemacht werden.

Denken Sie daran, dass durch das Löschen eines Agenten DataSync nicht dessen virtuelle Maschine (VM) oder EC2 Amazon-Instanz aus Ihrer Speicherumgebung entfernt wird. Sie können die VM oder Instanz löschen oder sie wiederverwenden, um einen neuen Agenten zu aktivieren.

Voraussetzungen

Löschen Sie einen Agenten erst, wenn Sie die DataSync Ressourcen, die von ihm abhängen, aktualisiert oder entfernt haben. Wenn Sie einen Agenten ersetzen, [aktualisieren Sie Ihre Transfer-Standorte](#) mit dem neuen Agenten. Wenn Sie keinen Agenten ersetzen, löschen Sie die [Übertragungsaufgaben](#) und [Standorte](#) zuerst mit diesem Agenten.

Den Agenten löschen

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Wählen Sie im linken Navigationsbereich die Option Kundendienstmitarbeiter aus.
3. Wählen Sie den Agenten aus, den Sie löschen möchten.
4. Wählen Sie Löschen, geben Sie den Text **delete** in das angezeigte Textfeld ein, und wählen Sie dann Löschen aus.
5. Wenn Sie nicht planen, die [Infrastruktur des Agenten für andere DataSync Aktivitäten wiederzuverwenden](#), löschen Sie die VM oder EC2 Amazon-Instance des Agenten, um sie aus Ihrer Speicherumgebung zu entfernen.

Die Infrastruktur eines DataSync Agenten wiederverwenden

Sie können eine Agentenressource aus der dem Agenten zugrunde liegenden VM oder EC2 Amazon-Instance löschen DataSync und trotzdem verwenden, um einen neuen Agenten zu aktivieren.

Um die Infrastruktur eines Agenten wiederzuverwenden

1. [Testen Sie die Verbindung des Agenten zu AWS](#). Wenn die Netzwerktests erfolgreich sind, fahren Sie mit dem nächsten Schritt fort.

Die Netzwerktests müssen bestanden werden, bevor Sie mit dem nächsten Schritt fortfahren können.

2. [Löschen Sie die Agentenressource](#) aus der VM oder EC2 Amazon-Instance des Agenten, DataSync aber löschen Sie nicht.
3. Wiederholen Sie Schritt 1, um die Verbindung des Agenten zu AWS erneut zu testen. Wenn die Netzwerktests erfolgreich sind, fahren Sie mit dem nächsten Schritt fort.
4. Überprüfen Sie etwa drei Minuten nach dem Löschen der Agentenressource von DataSync, ob Port 80 auf der Agenten-VM oder EC2 Amazon-Instance geöffnet ist. Wenn ja, fahren Sie mit dem nächsten Schritt fort.
5. [Aktivieren Sie einen neuen Agenten](#) mit der vorhandenen VM oder EC2 Amazon-Instance.

Sie können den neuen Agenten in einem anderen AWS-Region AWS-Konto, und mit einem anderen Typ von [Service-Endpoint](#) aktivieren. Wenn Sie einen anderen Typ von Service-Endpoint verwenden, müssen Sie Ihre [Netzwerkconfiguration](#) anpassen.

Löschen eines DataSync Standorts

Es hat sich bewährt, die AWS DataSync Standorte zu entfernen, die Sie nicht mehr benötigen.

Um einen Standort mithilfe der DataSync Konsole zu entfernen

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.
2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
3. Wählen Sie den Standort aus, den Sie entfernen möchten.
4. Wählen Sie Löschen aus. Bestätigen Sie den Löschvorgang, indem Sie die Eingabe eingebendelete, und wählen Sie dann Löschen.

Eine DataSync Aufgabe löschen

Wenn Sie eine AWS DataSync Aufgabe nicht mehr benötigen, können Sie sie und die zugehörigen AWS Ressourcen löschen.

Voraussetzungen

Wenn Sie eine Aufgabe ausführen, DataSync werden automatisch [Netzwerkschnittstellen](#) für den Datenübertragungsverkehr erstellt und verwaltet. Wenn Sie eine Aufgabe löschen, löschen Sie auch die zugehörigen Netzwerkschnittstellen, sofern Sie über die folgenden Berechtigungen verfügen:

- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:ModifyNetworkInterfaceAttribute

Diese Berechtigungen sind in der AWS verwalteten Richtlinie verfügbar `AWSDataSyncFullAccess`. Weitere Informationen finden Sie unter [AWS verwaltete Richtlinien für AWS DataSync](#).

Die Aufgabe wird gelöscht

Sobald Sie eine Aufgabe gelöscht haben, können Sie sie nicht wiederherstellen.

Verwenden der DataSync Konsole

1. Öffnen Sie die AWS DataSync Konsole unter <https://console.aws.amazon.com/datasync/>.

2. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Aufgaben aus.
3. Wählen Sie die Aufgabe aus, die Sie löschen möchten.
4. Wählen Sie Actions (Aktionen) und dann Delete (Löschen).
5. Wählen Sie im Dialogfeld (Bestätigung) Delete (Löschen) aus.

Mit dem AWS CLI

1. Kopieren Sie den folgenden `delete-task` Befehl:

```
aws datasync delete-task \  
    --task-arn "task-to-delete"
```

2. Geben Sie für den `--task-arn` Parameter den Amazon-Ressourcennamen (ARN) der Aufgabe an, die Sie löschen möchten (z. B. `arn:aws:datasync:us-east-2:123456789012:task/task-012345678abcd0123`).
3. Führen Sie den Befehl `delete-task` aus.

Sicherheit in AWS DataSync

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

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS -Compliance-Programme](#) regelmäßig. Informationen zu den Compliance-Programmen, die für AWS DataSync gelten, finden Sie unter [Vom Compliance-Programm abgedeckte AWS -Services](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. 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 hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können DataSync. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen DataSync, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer DataSync Ressourcen unterstützen.

Topics

- [Datenschutz in AWS DataSync](#)
- [Identitäts- und Zugriffsmanagement in AWS DataSync](#)
- [Konformitätsvalidierung für AWS DataSync](#)
- [Resilienz in AWS DataSync](#)
- [Infrastruktursicherheit in AWS DataSync](#)
- [Sicherung der Anmeldeinformationen für Speicherorte mit Secrets Manager](#)

Datenschutz in AWS DataSync

AWS DataSync überträgt Daten sicher zwischen selbstverwalteten Speichersystemen und AWS Speicherdiensten sowie zwischen AWS Speicherdiensten. Wie Ihre Speicherdaten bei der Übertragung verschlüsselt werden, hängt zum Teil von den an der Übertragung beteiligten Standorten ab.

Nach Abschluss der Übertragung werden die Daten im Ruhezustand durch das System oder den Dienst, der die Daten speichert, verschlüsselt (nicht DataSync).

Themen

- [AWS DataSync Verschlüsselung bei der Übertragung](#)
- [AWS DataSync Verschlüsselung im Ruhezustand](#)
- [Richtlinie für den Datenverkehr zwischen Netzwerken](#)

AWS DataSync Verschlüsselung bei der Übertragung

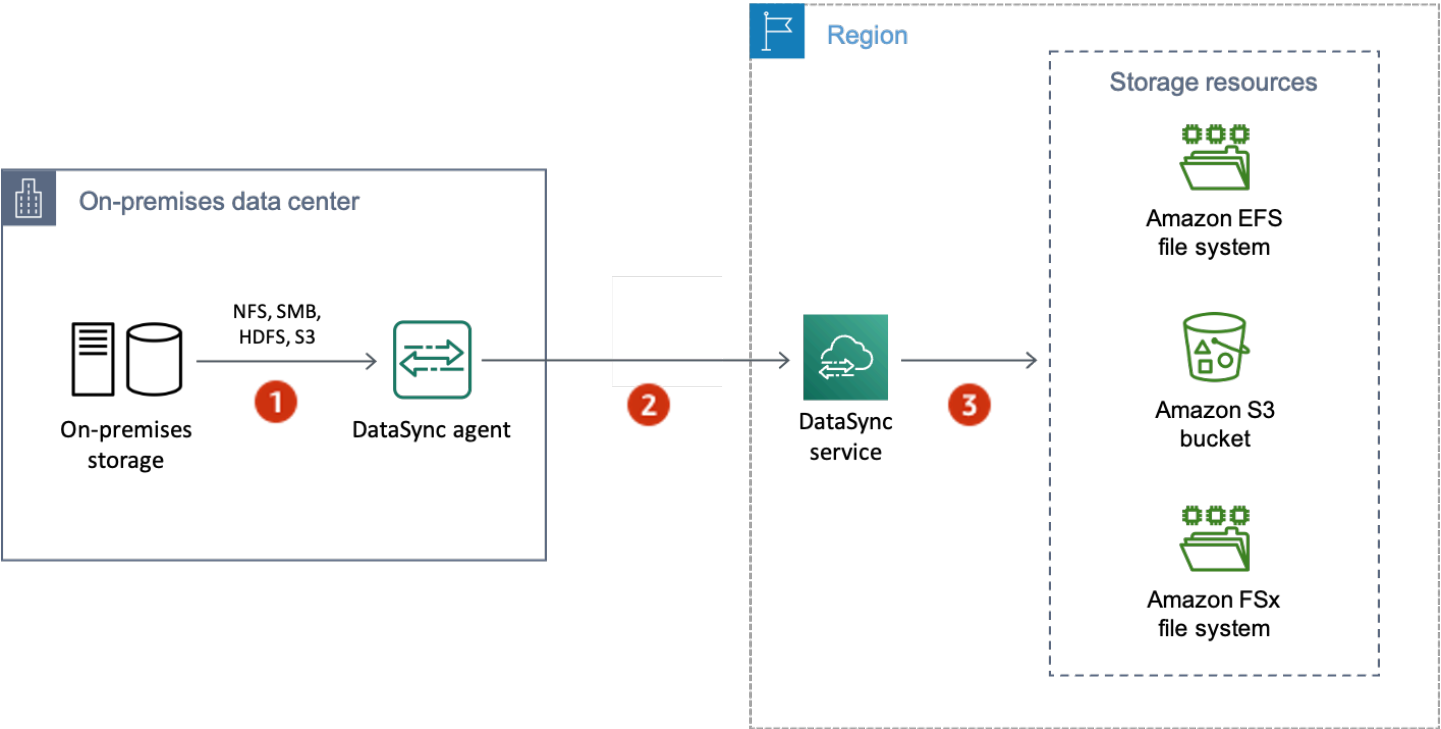
Ihre Speicherdaten (einschließlich Metadaten) werden bei der Übertragung verschlüsselt, aber wie sie während der Übertragung verschlüsselt werden, hängt von Ihren Quell- und Zielorten ab.

DataSync verwendet bei der Verbindung mit einem Standort die sichersten Optionen, die das Datenzugriffsprotokoll dieses Standorts bietet. Wenn Sie beispielsweise mithilfe von Server Message Block (SMB) eine Verbindung zu einem Dateisystem herstellen, werden die von SMB bereitgestellten Sicherheitsfunktionen DataSync verwendet.

Netzwerkverbindungen bei einer Übertragung

DataSync Zum Kopieren von Daten sind drei Netzwerkverbindungen erforderlich: eine Verbindung zum Lesen von Daten von einem Quellspeicherort, eine weitere zum Übertragen von Daten zwischen Standorten und eine weitere, um Daten an einen Zielort zu schreiben.

Das folgende Diagramm ist ein Beispiel für die Netzwerkverbindungen, die DataSync verwendet werden, um Daten von einem lokalen Speichersystem zu einem AWS Speicherdienst zu übertragen. Verwenden Sie die beigefügte Tabelle, um zu verstehen, wo die Verbindungen bestehen und wie die Daten bei der Übertragung über die einzelnen Verbindungen geschützt werden.



Referenz	Netzwerkverbindung	Beschreibung
1	Daten vom Quellspeicherort lesen	DataSync stellt eine Verbindung her, indem das Protokoll des Speichersystems für den Zugriff auf Daten verwendet wird (z. B. SMB oder die Amazon S3 S3-API). Bei dieser Verbindung werden die Daten mithilfe der Sicherheitsfunktionen des Speichersystems geschützt, sofern diese Funktionen DataSync nicht unterstützt werden. Unterstützt DataSync derzeit beispielsweise keine Kerberos-Authentifizierung mit NFS-Dateiservern oder wenn die TDE-Verschlüsselung mit HDFS verwendet wird.
2	Übertragung von Daten zwischen Standorten	DataSync Verschlüsselt für diese Verbindung den gesamten Netzwerkv

Referenz	Netzwerkverbindung	Beschreibung
		verkehr mit Mutual Transport Layer Security (mTLS) 1.3.
3	Daten werden an den Zielort geschrieben	Wie beim Quellspeicherort wird für die DataSync Verbindung das Protokoll des Speichersystems für den Datenzugriff verwendet. Daten werden wiederum mithilfe der Sicherheitsfunktionen des Speichersystems geschützt, sofern diese Funktionen DataSync nicht unterstützt werden.

Erfahren Sie, wie Ihre Daten bei der Übertragung verschlüsselt werden, wenn Sie DataSync eine Verbindung zu den folgenden AWS Speicherdiensten herstellen:

- [Amazon EFS](#)
- [Amazon FSx für Windows-Dateiserver](#)
- [Amazon FSx für Lustre](#)
- [Amazon FSx für OpenZFS](#)
- [Amazon FSx für NetApp ONTAP](#)
- [Amazon S3](#)

TLS-Verschlüsselungsverfahren

Verwendet bei der Übertragung von Daten zwischen DataSync Standorten unterschiedliche TLS-Chiffren. Die TLS-Verschlüsselung hängt von der Art des Dienstendpunkts ab, mit dem Ihr Agent kommuniziert. DataSync (Weitere Informationen finden Sie unter [Wählen Sie einen Service-Endpunkt für Ihren Agenten AWS DataSync.](#))

Inhalt

- [Öffentliche Endpunkte oder VPC-Endpunkte](#)
- [FIPS-Endpunkte](#)

Öffentliche Endpunkte oder VPC-Endpunkte

Verwendet für Public- und Virtual Private Cloud (VPC) DataSync -Dienstendpunkte eine der folgenden TLS-Chiffren:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_ (ECDH_x25519) SHA384
- TLS_ECDHE_RSA_WITH_0_05_ (ECDH_x25519CHACHA2) POLY13 SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_ (ECDH_x25519SHA256)

FIPS-Endpunkte

Verwendet für FIPS-Dienstendpunkte (Federal Information Processing Standard) die folgende TLS-Chiffre: DataSync

- TLS_AES_128_GCM_ (secp256r1) SHA256

AWS DataSync Verschlüsselung im Ruhezustand

Da es AWS DataSync sich um einen Übertragungsdienst handelt, werden Ihre Speicherdaten im Ruhezustand in der Regel nicht verwaltet. Die Speicherdienste und -systeme, die DataSync unterstützt werden, sind für den Schutz der Daten in diesem Zustand verantwortlich. Es gibt jedoch einige dienstbezogene Daten, die im Ruhezustand DataSync verwaltet werden.

Was ist verschlüsselt?

Die einzigen Daten, die im Ruhezustand DataSync verarbeitet werden, beziehen sich auf die Details, die für den Abschluss Ihrer Übertragung erforderlich sind. DataSync speichert die folgenden Daten mit vollständiger Verschlüsselung im Ruhezustand in Amazon DynamoDB:

- Aufgabenkonfigurationen (z. B. Details zu den Standorten in Ihrer Übertragung).
- Benutzeranmeldedaten, die es Ihrem DataSync Agenten ermöglichen, sich bei einem Standort zu authentifizieren. Diese Anmeldeinformationen werden mit den öffentlichen Schlüsseln Ihres Agenten verschlüsselt. Der Agent kann diese Schlüssel nach Bedarf mit seinen privaten Schlüsseln entschlüsseln.

Weitere Informationen finden Sie unter [DynamoDB-Verschlüsselung im Ruhezustand im](#) Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

Schlüsselverwaltung

Sie können die Verschlüsselungsschlüssel nicht verwalten, die zum Speichern von Informationen in DynamoDB DataSync verwendet werden, die sich auf die Ausführung Ihrer Aufgabe beziehen. Zu diesen Informationen gehören Ihre Aufgabenkonfigurationen und die Anmeldeinformationen, mit denen sich Agenten bei einem Speicherort authentifizieren.

Was ist nicht verschlüsselt?

DataSync Es hat zwar keine Kontrolle darüber, wie Ihre Speicherdaten im Ruhezustand verschlüsselt werden, wir empfehlen jedoch, Ihre Standorte mit der höchsten Sicherheitsstufe zu konfigurieren, die sie unterstützen. Sie können Objekte beispielsweise mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) oder (KMS) -Schlüsseln AWS Key Management Service (AWS SSE-KMS) verschlüsseln.

Erfahren Sie mehr darüber, wie AWS Speicherdienste Daten im Ruhezustand verschlüsseln:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Amazon FSx für Windows-Dateiserver](#)
- [Amazon FSx für Lustre](#)
- [Amazon FSx für OpenZFS](#)
- [Amazon FSx für NetApp ONTAP](#)

Richtlinie für den Datenverkehr zwischen Netzwerken

Wir empfehlen, Ihre Quell- und Zielstandorte mit der höchsten Sicherheitsstufe zu konfigurieren, die jeder Standort unterstützt. AWS DataSync Arbeitet bei der Verbindung mit einem Standort mit der sichersten Version des Datenzugriffsprotokolls, die das Speichersystem verwendet. Erwägen Sie außerdem, den Subnetzverkehr auf bekannte Protokolle und Dienste zu beschränken.

DataSync sichert die Verbindung zwischen Standorten — einschließlich zwischen AWS-Konten, AWS-Regionen und Availability Zones — mithilfe von Transport Layer Security (TLS) 1.3.

Identitäts- und Zugriffsmanagement in AWS DataSync

AWS verwendet Sicherheitsanmeldedaten, um Sie zu identifizieren und Ihnen Zugriff auf Ihre AWS Ressourcen zu gewähren. Sie können Funktionen von AWS Identity and Access

Management (IAM) verwenden, um anderen Benutzern, Diensten und Anwendungen die vollständige oder eingeschränkte Nutzung Ihrer AWS Ressourcen zu ermöglichen, ohne Ihre Sicherheitsanmeldeinformationen weiterzugeben.

Standardmäßig sind IAM-Identitäten (Benutzer, Gruppen und Rollen) nicht berechtigt, Ressourcen zu erstellen, anzuzeigen oder zu ändern. AWS Damit Benutzer, Gruppen und Rollen auf AWS DataSync Ressourcen zugreifen und mit der DataSync Konsole und der API interagieren können, empfehlen wir Ihnen, eine IAM-Richtlinie zu verwenden, die ihnen die Erlaubnis erteilt, die spezifischen Ressourcen und API-Aktionen zu verwenden, die sie benötigen. Anschließend hängen Sie die Richtlinie an die IAM-Identität an, die Zugriff erfordert. Eine Übersicht über die grundlegenden Elemente einer Richtlinie erhalten Sie unter [Zugriffsverwaltung für AWS DataSync](#).

Themen

- [Zugriffsverwaltung für AWS DataSync](#)
- [AWS verwaltete Richtlinien für AWS DataSync](#)
- [Vom Kunden verwaltete IAM-Richtlinien für AWS DataSync](#)
- [Verwenden von serviceverknüpften Rollen für DataSync](#)
- [Berechtigungen für das Markieren von DataSync Ressourcen während der Erstellung](#)
- [Serviceübergreifende Confused-Deputy-Prävention](#)

Zugriffsverwaltung für AWS DataSync

Jede AWS Ressource gehört einem AWS-Konto. Die Berechtigungen zum Erstellen einer Ressource oder für den Zugriff darauf werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann AWS Identity and Access Management (IAM-) Identitäten Berechtigungsrichtlinien zuordnen. Einige Dienste (z. B. AWS Lambda) unterstützen auch das Anhängen von Berechtigungsrichtlinien an Ressourcen.

Note

Ein Kontoadministrator ist ein Benutzer mit Administratorrechten in einem AWS-Konto. Weitere Informationen finden Sie unter [Bewährte Methoden für IAM](#) im IAM-Benutzerhandbuch.

Themen

- [DataSync Ressourcen und Operationen](#)
- [Grundlegendes zum Eigentum an Ressourcen](#)
- [Verwaltung des Zugriffs auf -Ressourcen](#)
- [Angaben der Richtlinienelemente: Aktionen, Effekte, Ressourcen und Prinzipale](#)
- [Angaben von Bedingungen in einer Richtlinie](#)
- [Erstellen einer VPC-Endpunktrichtlinie](#)

DataSync Ressourcen und Operationen

DataSyncIn sind die primären Ressourcen Agent, Standort, Aufgabe und Aufgabenausführung.

Diesen Ressourcen sind eindeutige Amazon-Ressourcennamen (ARNs) zugeordnet, wie in der folgenden Tabelle dargestellt.

Ressourc entyp	ARN-Format
ARN des Kundendie nstmitarb eiters	arn:aws:datasync: <i>region:account-id</i> :agent/ <i>agent-id</i>
Speicherort- ARN	arn:aws:datasync: <i>region:account-id</i> :location/ <i>location-id</i>
Aufgaben- ARN	arn:aws:datasync: <i>region:account-id</i> :task/ <i>task-id</i>
ARN für die Ausführun g von Aufgaben	arn:aws:datasync: <i>region:account-id</i> :task/ <i>task-id</i> /executio n/ <i>exec-id</i>

Um Berechtigungen für bestimmte API-Operationen, wie z. B. das Erstellen einer Aufgabe, zu gewähren, DataSync wird eine Reihe von Aktionen definiert, die Sie in einer Berechtigungsrichtlinie

angeben können. Für eine API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegendes zum Eigentum an Ressourcen

Ein Ressourcenbesitzer ist derjenige AWS-Konto, der die Ressource erstellt hat. Das heißt, der Ressourcenbesitzer ist derjenige AWS-Konto der Hauptentität (z. B. einer IAM-Rolle), die die Anfrage authentifiziert, mit der die Ressource erstellt wird. Die folgenden Beispiele veranschaulichen, wie dieses Verhalten funktioniert:

- Wenn Sie Ihre Root-Kontoanmeldeinformationen verwenden, AWS-Konto um eine Aufgabe zu erstellen, sind Sie AWS-Konto der Besitzer der Ressource (in DataSync, die Ressource ist die Aufgabe).
- Wenn Sie in Ihrem eine IAM-Rolle erstellen AWS-Konto und diesem Benutzer Berechtigungen für die `CreateTask` Aktion gewähren, kann der Benutzer eine Aufgabe erstellen. Ihre AWS-Konto, zu der der Benutzer gehört, besitzt jedoch die Aufgabenressource.
- Wenn Sie in Ihrem System eine IAM-Rolle AWS-Konto mit den Berechtigungen zum Erstellen einer Aufgabe erstellen, kann jeder, der die Rolle übernehmen kann, eine Aufgabe erstellen. Ihre AWS-Konto, zu der die Rolle gehört, besitzt die Aufgabenressource.

Verwaltung des Zugriffs auf -Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

Note

In diesem Abschnitt wird die Verwendung von IAM im Kontext von DataSync beschrieben. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter [Was ist IAM?](#) im IAM-Benutzerhandbuch. Informationen zur Syntax und Beschreibungen der IAM-Richtlinien finden Sie in der [AWS Identity and Access Management Richtlinienreferenz](#) im IAM-Benutzerhandbuch.

Mit einer IAM-Identität verknüpfte Richtlinien werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet, und Richtlinien, die einer Ressource zugeordnet sind, werden als ressourcenbasierte Richtlinien bezeichnet. DataSync unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- [Identitätsbasierte Richtlinien](#)
- [Ressourcenbasierte Richtlinien](#)

Identitätsbasierte Richtlinien

Sie können den DataSync Ressourcenzugriff mit IAM-Richtlinien verwalten. Diese Richtlinien können einem AWS-Konto Administrator dabei helfen, Folgendes zu tun: DataSync

- Berechtigungen zum Erstellen und Verwalten von DataSync Ressourcen gewähren — Erstellen Sie eine IAM-Richtlinie, die es einer IAM-Rolle in Ihrem Unternehmen ermöglicht, DataSync Ressourcen wie Agenten, Standorte und Aufgaben AWS-Konto zu erstellen und zu verwalten.
- Erteilen Sie Berechtigungen für eine Rolle in einer anderen AWS-Konto oder einer AWS-Service — Erstellen Sie eine IAM-Richtlinie, die Berechtigungen für eine IAM-Rolle in einer anderen oder einer gewährt. AWS-Konto AWS-Service Beispiel:
 1. Der Administrator von Konto A erstellt eine IAM-Rolle und fügt der Rolle, die Berechtigungen für Ressourcen in Konto A gewährt, eine Berechtigungsrichtlinie hinzu.
 2. Der Administrator von Konto A ordnet der Rolle eine Vertrauensrichtlinie zu, die Konto B als den Prinzipal identifiziert, der die Rolle übernehmen kann.

Um einem AWS-Service Benutzer die Berechtigung zur Übernahme der Rolle zu gewähren, kann der Administrator von Konto A in der Vertrauensrichtlinie an AWS-Service als Prinzipal angeben.

3. Der Administrator von Konto B kann dann die Berechtigungen zur Übernahme der Rolle an alle Benutzer in Konto B delegieren. Dadurch kann jeder, der die Rolle in Konto B verwendet, Ressourcen in Konto A erstellen oder darauf zugreifen.

Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter [Zugriffsverwaltung](#) im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie gewährt Berechtigungen für alle `List*` Aktionen auf allen Ressourcen. Diese Aktion ist schreibgeschützt und erlaubt keine Änderung von Ressourcen.

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowAllListActionsOnAllResources",
    "Effect": "Allow",
    "Action": [
      "datasync:List*"
    ],
    "Resource": "*"
  }
]
```

[Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit DataSync finden Sie unter AWS Verwaltete Richtlinien und Kundenverwaltete Richtlinien. Weitere Informationen zu IAM-Identitäten finden Sie im IAM-Benutzerhandbuch.](#)

Ressourcenbasierte Richtlinien

Andere Dienste, wie Amazon S3, unterstützen ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem Amazon S3-Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. Unterstützt jedoch DataSync keine ressourcenbasierten Richtlinien.

Angaben der Richtlinienelemente: Aktionen, Effekte, Ressourcen und Prinzipale

Für jede DataSync Ressource definiert der Dienst eine Reihe von API-Vorgängen (siehe [Aktionen](#)). DataSync Definiert eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können, um Berechtigungen für diese API-Operationen zu gewähren. Für die DataSync Ressource sind beispielsweise die folgenden Aktionen definiert: `CreateTask`, `DeleteTask`, und `DescribeTask`. Für das Durchführen einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- **Ressource** – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt. Für DataSync-Ressourcen können Sie das Platzhalterzeichen (`*`) in IAM-Richtlinien verwenden. Weitere Informationen finden Sie unter [DataSync Ressourcen und Operationen](#).
- **Aktion** – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Je nach dem angegebenen `Effect` Element gewährt oder verweigert

die `datasync:CreateTask` Berechtigung dem Benutzer beispielsweise die Berechtigungen zur Ausführung des DataSync `CreateTask` Vorgangs.

- **Effekt** — Sie geben den Effekt an, wenn der Benutzer die bestimmte Aktion anfordert. Dieser Effekt kann entweder `Allow` oder `Deny` sein. Wenn Sie nicht explizit Zugriff auf (`Allow`) auf eine Ressource gewähren, wird der Zugriff implizit verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern, um sicherzustellen, dass ein Benutzer nicht darauf zugreifen kann, auch wenn eine andere Richtlinie diesem Benutzer Zugriff gewährt. Weitere Informationen finden Sie unter [Autorisierung](#) im IAM-Benutzerhandbuch.
- **Prinzipal** – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. Bei ressourcenbasierten Richtlinien geben Sie den Benutzer, das Konto, den Dienst oder die andere Entität an, für die Sie Berechtigungen erhalten möchten (gilt nur für ressourcenbasierte Richtlinien). DataSync unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax und Beschreibung der IAM-Richtlinien finden Sie in der [AWS Identity and Access Management Richtlinienreferenz](#) im IAM-Benutzerhandbuch.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie beim Erteilen von Berechtigungen wirksam werden soll.

Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt.

Weitere Informationen zur Angabe von Bedingungen in der Richtliniensprache finden Sie unter [Bedingung](#) im IAM-Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Für DataSync gibt es keine speziellen Bedingungsschlüssel. Es gibt jedoch AWS umfangreiche Bedingungsschlüssel, die Sie je nach Bedarf verwenden können. Eine vollständige Liste der AWS Wide Keys finden Sie unter [Verfügbare Schlüssel](#) im IAM-Benutzerhandbuch.

Erstellen einer VPC-Endpunktrichtlinie

VPC-Endpunktrichtlinien helfen dabei, den Zugriff auf DataSync API-Operationen über DataSync VPC Dienstendpunkte und FIPS-fähige VPC-Dienstendpunkte zu kontrollieren. VPC-Endpunktrichtlinien ermöglichen es Ihnen, bestimmte DataSync API-Aktionen einzuschränken, auf die über Ihre VPC Service-Endpunkte zugegriffen wird, z. B. `CreateTask` oder `StartTaskExecution`.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf VPC-Endpoints mithilfe von Endpunktrichtlinien](#).

Beispielrichtlinie

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "datasync:CreateTask",
        "datasync:StartTaskExecution",
        "datasync:DescribeTask"
      ],
      "Resource": "arn:aws:datasync:us-east-1:123456789012:task/*"
    }
  ]
}
```

AWS verwaltete Richtlinien für AWS DataSync

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um [von Kunden verwaltete IAM-Richtlinien zu erstellen](#), die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter [AWS Verwaltete Richtlinien](#).

AWS-Services verwalten und aktualisieren Sie AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS

verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise nur Lesezugriff auf alle Ressourcen AWS-Services . Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in [Verwaltete AWS -Richtlinien für Auftragsfunktionen](#) im IAM-Leitfaden.

AWS verwaltete Richtlinie: `AWSDataSyncReadOnlyAccess`

Sie können die `AWSDataSyncReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt nur Leseberechtigungen für DataSync

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSDataSyncReadOnlyAccess](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: `AWSDataSyncFullAccess`

Sie können die `AWSDataSyncFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Administratorberechtigungen für den Dienst DataSync und ist für den AWS-Managementkonsole Zugriff darauf erforderlich. `AWSDataSyncFullAccess` bietet vollen Zugriff auf DataSync API-Operationen und die Operationen, die mit verwandten Ressourcen interagieren (wie Amazon S3 S3-Buckets, Amazon EFS-Dateisysteme, AWS KMS Schlüssel und Secrets Manager Manager-Geheimnisse). Die Richtlinie gewährt Amazon auch Berechtigungen CloudWatch, einschließlich der Erstellung von Protokollgruppen und der Erstellung oder Aktualisierung einer Ressourcenrichtlinie.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSDataSyncFullAccess](#) in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSDDataSyncServiceRolePolicy

Sie können die `AWSDDataSyncServiceRolePolicy` Richtlinie nicht an Ihre IAM-Identitäten anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, mit der Sie Aktionen DataSync in Ihrem Namen ausführen können. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für DataSync](#).

Diese Richtlinie gewährt Administratorberechtigungen, die es der serviceverknüpften Rolle ermöglichen, CloudWatch Amazon-Protokolle für DataSync Aufgaben im erweiterten Modus zu erstellen.

Richtlinienaktualisierungen

Änderungen	Beschreibung	Date
AWSDDataSyncFullAccess —Ändern	DataSync geänderte Genehmigungserklärungen für <code>AWSDDataSyncFullAccess</code> : Die aktualisierten Anweisungen entfernen Tagging-Bedingungen aus den Berechtigungen, die zum Erstellen von Secrets Manager Manager-Geheimnissen DataSync verwendet werden.	13. Mai 2025
AWSDDataSyncFullAccess —Ändern	DataSync neue Berechtigungen hinzugefügt für <code>AWSDDataSyncFullAccess</code> : <code>secretsmanager:CreateSecret</code> <code>secretsmanager:PutSecretValue</code>	7. Mai 2025

Änderungen	Beschreibung	Date
	• <code>secretsmanager:DeleteSecret</code> • <code>secretsmanager:UpdateSecret</code> Diese Berechtigungen ermöglichen das DataSync Erstellen, Bearbeiten und Löschen von AWS Secrets Manager Geheimnissen.	
AWSDataSyncFullAccess — Veränderung	DataSync neue Berechtigungen hinzugefügt für <code>AWSDataSyncFullAccess</code> : • <code>secretsmanager:ListSecrets</code> • <code>kms:ListAliases</code> • <code>kms:DescribeKey</code> Mit diesen Berechtigungen können Metadaten zu Ihren AWS Secrets Manager Geheimnissen und AWS KMS Schlüsseln DataSync abgerufen werden, einschließlich aller Aliase, die mit Ihren Schlüsseln verknüpft sind.	23. April 2025

Änderungen	Beschreibung	Date
AWSDataSyncServiceRolePolicy — Ändern	DataSync hat der <code>AWSDataSyncServiceRolePolicy</code> Richtlinie, die von der DataSync serviceverknüpften Rolle <code>AWSServiceRoleForDataSync</code> verwendet wird, neue Berechtigungen hinzugefügt: • <code>secretsmanager:DescribeSecret</code> • <code>secretsmanager:GetSecretValue</code> Diese Berechtigungen ermöglichen das DataSync Lesen von Metadaten und Werten für Geheimnisse, die von verwaltet werden AWS Secrets Manager.	15. April 2025
AWSDataSyncServiceRolePolicy – Neue Richtlinie	DataSync hat eine Richtlinie hinzugefügt, die von der DataSync serviceverknüpften Rolle <code>AWSServiceRoleForDataSync</code> verwendet wird. Diese neue verwaltete Richtlinie erstellt automatisch CloudWatch Amazon-Protokolle für Ihre DataSync Aufgaben, die den erweiterten Modus verwenden.	30. Oktober 2024

Änderungen	Beschreibung	Date
AWSDataSyncFullAccess — Ändern	DataSync hat eine neue Erlaubnis hinzugefügt für <code>AWSDataSyncFullAccess</code> : • <code>iam:CreateServiceLinkedRole</code> Mit dieser Berechtigung können DataSync Sie dienstbezogene Rollen für Sie erstellen.	30. Oktober 2024
AWSDataSyncFullAccess — Ändern	DataSync hat eine neue Erlaubnis hinzugefügt für <code>AWSDataSyncFullAccess</code> : • <code>ec2:DescribeRegions</code> Mit dieser Berechtigung können Sie beim Erstellen einer DataSync Aufgabe für Übertragungen zwischen AWS-Regionen diesen Regionen auswählen, für die Sie sich anmelden möchten.	22. Juli 2024

Änderungen	Beschreibung	Date
AWSDataSyncFullAccess — Ändern	DataSync hat eine neue Erlaubnis hinzugefügt für <code>AWSDataSyncFullAccess</code> : • <code>s3:ListBucketVersions</code> Mit dieser Berechtigung können Sie eine bestimmte Version Ihres DataSync Manifests auswählen.	16. Februar 2024

Änderungen	Beschreibung	Date
AWSDataSyncFullAccess — Ändern	DataSync neue Berechtigungen hinzugefügt für <code>AWSDataSyncFullAccess</code> : • <code>ec2:DescribeVpcEndpoints</code> • <code>elasticfilesystem:DescribeAccessPoints</code> • <code>fsx:DescribeStorageVirtualMachines</code> • <code>outposts:ListOutposts</code> • <code>s3:GetBucketLocation</code> • <code>s3-outposts:ListAccessPoints</code> • <code>s3-outposts:ListRegionalBuckets</code> Mit diesen Berechtigungen können Sie DataSync Agenten und Standorte für Amazon EFS, Amazon FSx for NetApp ONTAP, Amazon S3 und S3 auf Outposts erstellen.	2. Mai 2023
DataSync hat begonnen, Änderungen zu verfolgen	DataSync hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	1. März 2021

Vom Kunden verwaltete IAM-Richtlinien für AWS DataSync

Zusätzlich zu AWS verwalteten Richtlinien können Sie auch Ihre eigenen identitätsbasierten Richtlinien für die (IAM-) Identitäten erstellen und diese an die AWS Identity and Access Management (IAM AWS DataSync -) Identitäten anhängen, für die diese Berechtigungen erforderlich sind. Diese werden als vom Kunden verwaltete Richtlinien bezeichnet. Dabei handelt es sich um eigenständige Richtlinien, die Sie selbst verwalten. AWS-Konto

Important

Bevor Sie beginnen, empfehlen wir Ihnen, sich mit den grundlegenden Konzepten und Optionen für die Verwaltung des Zugriffs auf Ihre DataSync Ressourcen vertraut zu machen. Weitere Informationen finden Sie unter [Zugriffsverwaltung für AWS DataSync](#).

Wenn Sie eine vom Kunden verwaltete Richtlinie erstellen, fügen Sie Aussagen zu DataSync Vorgängen bei, die für bestimmte AWS Ressourcen verwendet werden können. Die folgende Beispielrichtlinie besteht aus zwei Aussagen (beachten Sie die Resource Elemente Action und in jeder Anweisung):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsSpecifiedActionsOnAllTasks",
      "Effect": "Allow",
      "Action": "datasync:DescribeTask",
      "Resource": "arn:aws:datasync:us-east-1:111122223333:task/*"
    },
    {
      "Sid": "ListAllTasks",
      "Effect": "Allow",
      "Action": "datasync:ListTasks",
      "Resource": "*"
    }
  ]
}
```

Die Aussagen der Richtlinie haben folgende Auswirkungen:

- Die erste Anweisung erteilt Berechtigungen zur Ausführung der `datasync:DescribeTask` Aktion für bestimmte Ressourcen der Übertragungsaufgabe, indem ein Amazon-Ressourcenname (ARN) mit einem Platzhalterzeichen (*) angegeben wird.
- Die zweite Anweisung erteilt Berechtigungen zur Ausführung der `datasync:ListTasks` Aktion für alle Aufgaben, indem nur ein Platzhalterzeichen (*) angegeben wird.

Beispiele für vom Kunden verwaltete Richtlinien

Das folgende Beispiel für vom Kunden verwaltete Richtlinien gewährt Berechtigungen für verschiedene DataSync Vorgänge. Die Richtlinien funktionieren, wenn Sie das AWS Command Line Interface (AWS CLI) oder ein AWS SDK verwenden. Um diese Richtlinien in der Konsole zu verwenden, müssen Sie auch die verwaltete Richtlinie verwenden `AWSDataSyncFullAccess`.

Themen

- [Beispiel 1: Erstellen Sie eine Vertrauensbeziehung, die DataSync den Zugriff auf Ihren Amazon S3 S3-Bucket ermöglicht](#)
- [Beispiel 2: Lese- und DataSync Schreibzugriff auf Ihren Amazon S3 S3-Bucket zulassen](#)
- [Beispiel 3: Erlauben DataSync Sie das Hochladen von Protokollen in CloudWatch Protokollgruppen](#)

Beispiel 1: Erstellen Sie eine Vertrauensbeziehung, die DataSync den Zugriff auf Ihren Amazon S3 S3-Bucket ermöglicht

Das Folgende ist ein Beispiel für eine Vertrauensrichtlinie, die es ermöglicht, eine IAM-Rolle DataSync zu übernehmen. Diese Rolle ermöglicht DataSync den Zugriff auf einen Amazon S3 S3-Bucket. Um das [dienstübergreifende Problem der verwirrten Deputy](#) zu vermeiden, empfehlen wir, die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in der Richtlinie zu verwenden.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

        "Principal": {
            "Service": "datasync.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "111111111111"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws:datasync:us-east-1:111111111111:*"
            }
        }
    }
}

```

Beispiel 2: Lese- und DataSync Schreibzugriff auf Ihren Amazon S3 S3-Bucket zulassen

Die folgende Beispielrichtlinie gewährt DataSync die Mindestberechtigungen zum Lesen und Schreiben von Daten in einen S3-Bucket, der als Zielort verwendet wird.

Note

Der Wert für `aws:ResourceAccount` sollte die Konto-ID sein, der der in der Richtlinie angegebene Amazon S3 S3-Bucket gehört.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {

```

```

        "aws:ResourceAccount": "123456789012"
    }
}
},
{
    "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectTagging"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "123456789012"
        }
    }
}
]
}

```

Beispiel 3: Erlauben DataSync Sie das Hochladen von Protokollen in CloudWatch Protokollgruppen

DataSync benötigt Berechtigungen, um Protokolle in Ihre CloudWatch Amazon-Protokollgruppen hochladen zu können. Sie können CloudWatch Protokollgruppen verwenden, um Ihre Aufgaben zu überwachen und zu debuggen.

Ein Beispiel für eine IAM-Richtlinie, die solche Berechtigungen gewährt, finden Sie unter. [Ermöglicht DataSync das Hochladen von Protokollen in eine CloudWatch Protokollgruppe](#)

Verwenden von serviceverknüpften Rollen für DataSync

AWS DataSync verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. DataSync Mit Diensten verknüpfte Rollen sind vordefiniert DataSync und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Themen

- [Rollen verwenden für DataSync](#)

Rollen verwenden für DataSync

AWS DataSync verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. DataSync mit Diensten verknüpfte Rollen sind vordefiniert DataSync und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle DataSync erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. DataSync definiert die Berechtigungen ihrer dienstbezogenen Rollen und DataSync kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre DataSync Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

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

Berechtigungen für dienstverknüpfte Rollen DataSync

DataSync verwendet die dienstgebundene Rolle mit dem Namen `AWSServiceRoleForDataSync`—Ermöglicht DataSync die Ausführung wichtiger Operationen zur Ausführung von Übertragungsaufgaben, einschließlich des Lesens von AWS Secrets Manager Geheimnissen und der Erstellung von CloudWatch Protokollgruppen und Ereignissen.

Die `AWSServiceRoleForDataSync` dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `datasync.amazonaws.com`

Die dienstverknüpfte Rolle verwendet die angegebene AWS verwaltete Richtlinie [AWSDataSyncServiceRolePolicy](#), mit der die folgenden Aktionen DataSync für die angegebenen Ressourcen ausgeführt werden können:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCloudWatchLogCreateAccess",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Sid": "DataSyncCloudWatchLogStreamUpdateAccess",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/datasync*:log-stream:*"
      ]
    },
    {
      "Sid": "DataSyncSecretsManagerReadAccess",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition": {
        "StringEquals": {

```

```
        "secretsmanager:ResourceTag/  
aws:secretsmanager:owningService": "aws-datasync",  
        "aws:ResourceAccount": "${aws:PrincipalAccount}"  
    }  
  }  
}  
]  
}
```

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für DataSync

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine DataSync Aufgabe in der AWS-Managementkonsole, der oder der AWS API erstellen AWS CLI, DataSync wird die dienstbezogene Rolle für Sie erstellt.

In der AWS CLI oder der AWS API können Sie eine dienstbezogene Rolle mit dem `datasync.amazonaws.com` Dienstnamen erstellen. Weitere Informationen finden Sie unter [Erstellen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

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 eine DataSync Aufgabe erstellen, DataSync wird die dienstbezogene Rolle erneut für Sie erstellt.

Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben IAM-Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für DataSync

DataSync erlaubt es Ihnen nicht, die `AWSServiceRoleForDataSync` dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für DataSync

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 Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

Note

Wenn der DataSync Dienst 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.

Um DataSync Ressourcen zu löschen, die verwendet werden von AWSService RoleForDataSync

1. [Löschen Sie die von der Aufgabe verwendeten DataSync Agenten](#) (falls vorhanden).
2. [Löscht die Speicherorte der Aufgabe.](#)
3. [Löscht die Aufgabe.](#)

Manuelles Löschen der serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleForDataSync serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte DataSync-Rollen

DataSync unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [AWS -Regionen und Endpunkte](#).

Berechtigungen für das Markieren von DataSync Ressourcen während der Erstellung

Bei einigen AWS DataSync API-Aktionen zur Ressourcenerstellung können Sie Tags angeben, wenn Sie die Ressource erstellen. Sie können Ressourcen-Tags verwenden, um die attributbasierte Zugriffskontrolle (ABAC) zu implementieren. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Damit Benutzer Ressourcen bei der Erstellung taggen können, müssen sie über Berechtigungen zur Verwendung der Aktion verfügen, mit der die Ressource erstellt wird (z. B. `datasync:CreateAgent` oder `datasync:CreateTask`). Wenn bei der Aktion zum Erstellen der Ressource Tags angegeben werden, müssen Benutzer auch über ausdrückliche Berechtigungen zur Verwendung der `datasync:TagResource` Aktion verfügen.

Die `datasync:TagResource`-Aktion wird nur ausgewertet, wenn die Tags während der Aktion zur Ressourcenerstellung angewendet werden. Daher benötigt ein Benutzer, der berechtigt ist, eine Ressource zu erstellen (vorausgesetzt, es gibt keine Tagging-Bedingungen), keine Berechtigungen, um die `datasync:TagResource` Aktion zu verwenden, wenn in der Anforderung keine Tags angegeben sind.

Wenn der Benutzer jedoch versucht, eine Ressource mit Tags zu erstellen, schlägt die Anforderung fehl, wenn der Benutzer nicht über die erforderlichen Berechtigungen zur Verwendung der `datasync:TagResource` Aktion verfügt.

Beispiele für IAM-Richtlinienerklärungen

Verwenden Sie die folgenden Beispiele für IAM-Richtlinienanweisungen, um Benutzern `TagResource` Berechtigungen zu erteilen, die Ressourcen erstellen DataSync .

Die folgende Anweisung ermöglicht es Benutzern, einen DataSync Agenten zu taggen, wenn sie den Agenten erstellen.

JSON

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

```

        "Effect": "Allow",
        "Action": "datasync:TagResource",
        "Resource": "arn:aws:datasync:us-east-1:444455556666:agent/*"
    }
]
}

```

Die folgende Anweisung ermöglicht es Benutzern, einen DataSync Standort zu taggen, wenn sie den Standort erstellen.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "datasync:TagResource",
      "Resource": "arn:aws:datasync:us-east-1:111122223333:location/*"
    }
  ]
}

```

Die folgende Anweisung ermöglicht es Benutzern, eine DataSync Aufgabe zu taggen, wenn sie die Aufgabe erstellen.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "datasync:TagResource",
      "Resource": "arn:aws:datasync:us-east-1:444455556666:task/*"
    }
  ]
}

```

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiere Entität zur Durchführung der Aktion zwingen kann. In AWS, dienststellenübergreifender Identitätswechsel kann zum Problem des verwirrten Stellvertreters führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel [aws:SourceArn](#) und die [aws:SourceAccount](#) globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS DataSync Ressource einen anderen Dienst gewähren. Wenn Sie beide globale Bedingungskontextschlüssel verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie diese Option, `aws:SourceAccount` wenn Sie möchten, dass eine Ressource in diesem Konto der dienstübergreifenden Nutzung zugeordnet wird.

Der Wert von `aws:SourceArn` muss den DataSync Standort-ARN enthalten, mit dem die DataSync IAM-Rolle übernommen werden darf.

Der effektivste Weg, sich vor dem Problem des verwirrten Stellvertreters zu schützen, besteht darin, den `aws:SourceArn` Schlüssel mit dem vollständigen ARN der Ressource zu verwenden. Wenn Sie den vollständigen ARN nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie Platzhalterzeichen (*) für die unbekannten Teile. Hier sind einige Beispiele dafür, wie Sie dies tun können für DataSync:

- Um die Vertrauensrichtlinie auf einen vorhandenen DataSync Standort zu beschränken, nehmen Sie den vollständigen Standort-ARN in die Richtlinie auf. DataSync übernimmt die IAM-Rolle nur, wenn es um diesen bestimmten Standort geht.
- Wenn Sie einen Amazon S3 S3-Standort für erstellen DataSync, kennen Sie den ARN des Standorts nicht. Verwenden Sie in diesen Szenarien das folgende Format für den `aws:SourceArn` Schlüssel: `arn:aws:datasync:us-east-2:123456789012:*`. Dieses Format validiert die Partition (aws), die Konto-ID und die Region.

Das folgende vollständige Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung in einer Vertrauensrichtlinie verwenden können, um das Problem mit DataSync dem verwirrten Stellvertreter zu vermeiden.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:datasync:us-east-2:123456789012:*"
        }
      }
    }
  ]
}
```

Weitere Beispielrichtlinien, die zeigen, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel mit verwenden können DataSync, finden Sie in den folgenden Themen:

- [Erstellen Sie eine Vertrauensbeziehung, die DataSync den Zugriff auf Ihren Amazon S3 S3-Bucket ermöglicht](#)
- [Konfigurieren Sie eine IAM-Rolle für den Zugriff auf Ihren Amazon S3 S3-Bucket](#)

Konformitätsvalidierung für AWS DataSync

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt](#), finden Sie unter [Umfang nach Compliance-Programm AWS-Services](#)

[unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der [AWS Sicherheitsdokumentation](#).

Resilienz in AWS DataSync

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Note

Wenn eine Availability Zone, in die Sie Daten migrieren oder aus der Sie Daten migrieren, während Sie eine DataSync Aufgabe ausführen, schlägt auch die Aufgabe fehl.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Infrastruktursicherheit in AWS DataSync

Als verwalteter Service AWS DataSync ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff DataSync über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Sicherung der Anmeldeinformationen für Speicherorte mit Secrets Manager

Note

Die Secrets Manager Manager-Integration ist für Objektspeicher und Microsoft Azure Blob Storage verfügbar.

DataSync verwendet [Standorte](#), um auf Ihre Speicherressourcen zuzugreifen, die sich vor Ort, in anderen Clouds oder in AWS befinden. Bei einigen Standorttypen müssen Sie Anmeldeinformationen angeben, z. B. einen Zugriffsschlüssel und einen geheimen Schlüssel oder einen Benutzernamen und ein Passwort, um sich bei Ihrem Speichersystem zu authentifizieren. Wenn Sie einen DataSync Standort erstellen, für den Anmeldeinformationen für die Authentifizierung erforderlich sind, können Sie AWS Secrets Manager (Secrets Manager) verwenden, um das Geheimnis für Ihre Anmeldeinformationen zu speichern. Die folgenden Optionen sind verfügbar:

- Speichern Sie das Geheimnis in Secrets Manager, indem Sie ein vom Service verwaltetes Geheimnis verwenden, das mit einem Standardschlüssel verschlüsselt ist.
- Speichern Sie das Geheimnis in Secrets Manager, indem Sie ein vom Service verwaltetes Geheimnis verwenden, das mit einem von Ihnen verwalteten AWS KMS Schlüssel verschlüsselt ist.
- Speichern Sie das Geheimnis in Secrets Manager mithilfe eines Secrets und Schlüssels, den Sie erstellen und verwalten. DataSync greift mithilfe einer von Ihnen bereitgestellten IAM-Rolle auf dieses Geheimnis zu.

In allen Fällen wird das Secrets Manager Manager-Geheimnis in Ihrem Konto gespeichert, sodass Sie das Geheimnis bei Bedarf unabhängig vom DataSync Dienst aktualisieren können. Secrets, die von erstellt und verwaltet werden DataSync , haben das Präfixaws-datasync.

Die Verwendung von Geheimnissen wird Ihnen nur dann in Rechnung gestellt, wenn Sie Geheimnisse außerhalb von Diensten erstellen DataSync oder API-Aufrufe für vom Dienst verwaltete Geheimnisse aus anderen Diensten als DataSync ausführen.

Verwenden eines vom Service verwalteten Geheimnisses, das mit einem Standardschlüssel verschlüsselt ist

Wenn Sie Ihren DataSync Standort erstellen, geben Sie einfach die geheime Zeichenfolge an. DataSyncerstellt eine geheime Ressource in Secrets Manager, um das von Ihnen angegebene Geheimnis zu speichern, und verschlüsselt das Geheimnis mit dem standardmäßigen Secrets Manager KMS-Schlüssel für Ihr Konto. Sie können den geheimen Wert direkt in Secrets Manager ändern oder indem Sie den Speicherort mithilfe der DataSync Konsole oder des SDK aktualisieren. AWS CLI Wenn Sie die Standortressource löschen oder sie so aktualisieren, dass sie ein benutzerdefiniertes Geheimnis verwendet, wird die geheime Ressource automatisch DataSync gelöscht.

Note

Um geheime Ressourcen in Secrets Manager zu erstellen, zu ändern und zu löschen, DataSync müssen Sie über die entsprechenden Berechtigungen verfügen. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien für DataSync](#).

Es wird ein vom Service verwaltetes Geheimnis verwendet, das mit einem benutzerdefinierten AWS KMS Schlüssel verschlüsselt ist

Wenn Sie Ihren DataSync Standort erstellen, geben Sie das Geheimnis und den ARN Ihres AWS KMS Schlüssels an. DataSync erstellt automatisch eine geheime Ressource in Secrets Manager, um das von Ihnen angegebene Geheimnis zu speichern, und verschlüsselt es mit Ihrem AWS KMS Schlüssel. Sie können den geheimen Wert direkt in Secrets Manager ändern oder indem Sie den Speicherort mithilfe der DataSync Konsole oder des SDK aktualisieren. AWS CLI Wenn Sie die Standortressource löschen oder sie so aktualisieren, dass sie ein benutzerdefiniertes Geheimnis verwendet, wird die geheime Ressource automatisch DataSync gelöscht.

Note

Ihr AWS KMS Schlüssel muss eine symmetrische Verschlüsselung mit dem ENCRYPT_DECRYPT Schlüsseltyp verwenden. Weitere Informationen finden Sie im AWS Secrets Manager Benutzerhandbuch unter [Einen AWS Key Management Service Schlüssel auswählen](#).

Um geheime Ressourcen in Secrets Manager zu erstellen, zu ändern und zu löschen, DataSync müssen Sie über die entsprechenden Berechtigungen verfügen. Weitere Informationen finden Sie unter [AWS managed policy: AWSDDataSyncFullAccess](#) (verwaltete Richtlinie).

Neben der Verwendung der richtigen DataSync verwalteten Richtlinie benötigen Sie auch die folgenden Berechtigungen:

```
{
  "Sid": "DataSyncKmsPermissions",
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "your-kms-key-arn",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "secretsmanager.*.amazonaws.com"
    }
  }
}
```

your-kms-key-arn Ersetzen Sie es durch Ihren KMS-Schlüssel ARN.

Um den geheimen Wert abzurufen und zu entschlüsseln, DataSync verwendet eine Service Linked Role (SLR), um auf Ihren AWS KMS Schlüssel zuzugreifen. Um sicherzustellen, dass Sie Ihren KMS-Schlüssel verwenden DataSync können, fügen Sie der Richtlinienerklärung des Schlüssels Folgendes hinzu:

```
{
  "Sid": "Allow DataSync to use the key for decryption",
```

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

Ersetze es **111122223333** durch deine AWS-Konto ID.

Verwenden Sie ein Geheimnis, das Sie verwalten

Bevor Sie Ihren DataSync Standort erstellen, [erstellen Sie ein Geheimnis in Secrets Manager](#). Der Wert für das Geheimnis darf nur die geheime Zeichenfolge selbst im Klartext enthalten. Wenn Sie Ihren DataSync Standort erstellen, geben Sie den ARN Ihres Geheimnisses und eine IAM-Rolle an, die DataSync für den Zugriff auf Ihr Geheimnis und den AWS KMS Schlüssel verwendet wird, mit dem Ihr Geheimnis verschlüsselt wurde. Gehen Sie wie folgt vor, um eine IAM-Rolle mit den entsprechenden Berechtigungen zu erstellen:

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen und dann Rolle erstellen aus.
3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option AWS Dienst aus.
4. Wählen Sie unter Anwendungsfall eine Option DataSyncaus der Dropdownliste aus. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus. Geben Sie einen Namen für Ihre Rolle ein und wählen Sie dann Rolle erstellen aus.
6. Suchen Sie auf der Seite Rollen nach der Rolle, die Sie gerade erstellt haben, und wählen Sie ihren Namen aus.
7. Wählen Sie auf der Detailseite für die Rolle den Tab Berechtigungen aus. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
8. Wählen Sie die Registerkarte JSON und fügen Sie dem Richtlinieneditor die folgenden Berechtigungen hinzu:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:your-secret-name"
    }
  ]
}
```

your-secret-name Ersetzen Sie es durch den Namen Ihres Secrets Manager Manager-Geheimnisses.

9. Wählen Sie Weiter aus. Geben Sie einen Namen für Ihre Richtlinie ein und wählen Sie dann Richtlinie erstellen aus.
10. (Empfohlen) Gehen Sie wie folgt vor, um das [dienstübergreifende Problem mit verwirrten Stellvertretern](#) zu vermeiden:
 - a. Wählen Sie auf der Detailseite für die Rolle die Registerkarte Vertrauensbeziehungen aus. Wählen Sie Vertrauensrichtlinie bearbeiten aus.
 - b. Aktualisieren Sie die Vertrauensrichtlinie anhand des folgenden Beispiels, das die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel enthält:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

        "Principal": {
            "Service": "datasync.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws:datasync:us-
east-1:111122223333:*"
            }
        }
    }
}

```

c. Wählen Sie Richtlinie aktualisieren.

Sie können diese Rolle bei der Erstellung Ihres Standorts angeben. Wenn Ihr Secret einen vom Kunden verwalteten AWS KMS Schlüssel für die Verschlüsselung verwendet, müssen Sie auch die Richtlinie des Schlüssels aktualisieren, um den Zugriff von der Rolle aus zu ermöglichen, die Sie im vorherigen Verfahren erstellt haben. Um die Richtlinie zu aktualisieren, fügen Sie der Richtlinienerklärung Ihres AWS KMS Schlüssels Folgendes hinzu:

```

{
    "Sid": "Allow DataSync use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam:111122223333:role/your-role-name"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}

```

111122223333 Ersetzen Sie es durch Ihre AWS-Konto ID und **your-role-name** den Namen der IAM-Rolle, die Sie im vorherigen Verfahren erstellt haben.

 Note

Wenn Sie Geheimnisse im Secrets Manager speichern, AWS-Konto fallen Gebühren an. Informationen zu Preisen erhalten Sie unter [AWS Secrets Manager -Preise](#).

AWS DataSync Kontingente

Informieren Sie sich über Ressourcenkontingente und -beschränkungen bei der Arbeit mit AWS DataSync.

Speichersystem-, Datei- und Objektbeschränkungen

In der folgenden Tabelle werden die DataSync Grenzwerte beschrieben, die bei der Arbeit mit Speichersystemen, Dateien und Objekten gelten.

Beschreibung	Limit
Maximale Gesamtlänge des Dateipfads	4,096 Bytes
Maximale Länge der Dateipfadkomponente (Dateiname, Verzeichnis oder Unterverzeichnis)	255 Byte
Maximale Länge der Windows-Domäne	253 Zeichen
Maximale Länge des Server-Hostnamens	255 Zeichen
Maximale Länge des Amazon S3 S3-Objektnamens	1.024 UTF-8-Zeichen

DataSync Kontingente

In der folgenden Tabelle werden die Kontingente für DataSync Ressourcen in einer bestimmten AWS-Konto Region beschrieben.

Ressource	Kontingent	Einstellbar
Maximale Anzahl von Aufgaben, die Sie erstellen können	100	Ja
(Aufgaben im erweiterten Modus) Maximale Anzahl von Quell- und Zielobjekten, mit denen	Praktisch unbegrenzt	N/A

Ressource	Kontingent	Einstellbar
pro Aufgabenausführung gearbeitet werden DataSync kann Weitere Informationen finden Sie unter Wie werden Dateien, Objekte und Verzeichnisse DataSync übertragen.		

Ressource	Kontingent	Einstellbar
(Aufgaben im Basismodus) Maximale Anzahl von Quell- und Zielfordateien, Objekten und Verzeichnissen, mit DataSync denen pro Aufgabenausführung zwischen lokalen, selbstverwalteten oder anderen Cloud-Speicher- und AWS Speicherdiensten gearbeitet werden kann Weitere Informationen finden Sie unter Wie werden Dateien, Objekte und Verzeichnisse DataSync übertragen.	50 Millionen  Important Denken Sie bei diesem Kontingent an Folgendes: • Wenn Sie Amazon S3 S3-Objekte mit Präfixen übertragen, werden die Präfixe als Verzeichnisse behandelt und auf das Kontingent angerechnet. DataSync Ich würde das zum Beispiel <code>s3://bucket/foo/bar.txt</code> als zwei Verzeichnisse (<code>./</code> und <code>./foo/</code>) und ein Objekt (<code>bar.txt</code>) betrachten. • Wenn Ihre Aufgabe mit mehr als 20 Millionen Dateien, Objekten oder Verzeichnissen arbeitet, stellen Sie sicher, dass Sie Ihrem DataSync Agenten mindestens 64 GB RAM	Ja  Tip Anstatt eine Erhöhung zu beantragen, können Sie mithilfe von Ein- und Ausschlussfiltern Aufgaben erstellen, die sich auf bestimmte Verzeichnisse konzentrieren. Weitere Informationen finden Sie unter Filtern

Ressource	Kontingent	Einstellbar
	zuweisen. Weitere Informationen finden Sie unter Agentenanforderungen für DataSync Übertragungen .	der übertragenen Daten von DataSync.

Ressource	Kontingent	Einstellbar
(Aufgaben im Basismodus) Maximale Anzahl von Quell- und Zielfordateien, Objekten und Verzeichnissen, mit denen pro Aufgabenausführung zwischen AWS Speicherdiensten gearbeitet werden DataSync kann Weitere Informationen finden Sie unter Wie werden Dateien, Objekte und Verzeichnisse DataSync übertragen.	25 Millionen  Important Wenn Sie Amazon S3 S3-Objekte mit Präfixen übertragen, werden die Präfixe als Verzeichnisse behandelt und auf das Kontingent angerechnet. DataSync Ich würde das zum Beispiel s3://bucket/foo/bar.txt als zwei Verzeichnisse (./und ./foo/) und ein Objekt (bar.txt) betrachten.	Ja  Tip Anstatt eine Erhöhung anzufordern, können Sie mithilfe von Ein- und Ausschlussfiltern Aufgaben erstellen, die sich auf bestimmte Verzeichnisse konzentrieren. Weitere Informationen finden Sie unter Filtern der

Ressource	Kontingent	Einstellbar
		übertragen Daten von DataSync.
Maximaler Durchsatz pro Aufgabe (für Übertragungen, bei denen ein DataSync Agent verwendet wird)	10 Gbit/s	Nein
Maximaler Durchsatz pro Aufgabe (für Übertragungen, bei denen kein DataSync Agent verwendet wird)	5 Gbit/s	Nein
Maximale Anzahl von Zeichen, die Sie in einen Aufgabenfilter aufnehmen können	102.400 Zeichen	Nein
	 Note Wenn Sie die DataSync Konsole verwenden, umfasst dieses Limit alle Zeichen, die in Ihren Ein- und Ausschlussmustern zusammengefasst sind.	
Maximale Anzahl von Ausführungen in der Warteschlange für eine einzelne Aufgabe	50	Nein
Maximale Anzahl gleichzeitiger Aufgabenausführungen im erweiterten Modus	120	Nein

Ressource	Kontingent	Einstellbar
Maximale Anzahl von Tagen, an denen der Verlauf einer Aufgabenausführung aufbewahrt wird	30	Nein
Maximale Größe für eine Manifestdatei mit Aufgaben im erweiterten Modus	20 GB	Nein

Anfordern einer Kontingenterhöhung

Für einige DataSync Kontingente können Sie eine Erhöhung beantragen. Erhöhungen werden nicht sofort gewährt und es kann einige Tage dauern, bis sie wirksam werden.

So fordern Sie eine Kontingenterhöhung an

1. Öffnen Sie die Service Quotas-Konsole unter <https://console.aws.amazon.com/servicequotas/>.
2. Wählen Sie im Navigationsbereich AWS Dienste und dann aus AWS DataSync.
3. Wählen Sie das Kontingent aus, das Sie erhöhen möchten, und wählen Sie dann Erhöhung auf Kontoebene beantragen aus.
4. Geben Sie den Gesamtbetrag ein, auf den sich das Kontingent belaufen soll, und wählen Sie dann „Beantragen“.

Wenn Sie ein anderes Kontingent erhöhen müssen, füllen Sie eine separate Anfrage aus.

AWS DataSync Probleme beheben

Verwenden Sie die folgenden Informationen, um AWS DataSync Probleme und Fehler zu beheben.

Themen

- [Behebung von Problemen mit DataSync Agenten](#)
- [Behebung von Problemen mit DataSync Standorten](#)
- [Behebung von Problemen mit DataSync Aufgaben](#)
- [Behebung von Problemen mit der Datenüberprüfung](#)
- [Fehlerbehebung bei höheren als erwarteten S3-Speicherkosten mit DataSync](#)

Behebung von Problemen mit DataSync Agenten

Verwenden Sie die folgenden Informationen, um Probleme mit AWS DataSync Agenten zu beheben. Zu diesen Problemen können gehören:

- Probleme beim Herstellen einer Verbindung zur lokalen Konsole eines EC2 Amazon-Agenten
- Der Aktivierungsschlüssel eines Agenten konnte nicht abgerufen werden
- Probleme bei der Aktivierung eines Agenten mit einem VPC-Serviceendpunkt
- Es wird festgestellt, dass ein Agent offline ist

Wie stelle ich eine Verbindung zur lokalen Konsole eines EC2 Amazon-Agenten her?

Um eine Verbindung zur lokalen Konsole eines EC2 Amazon-Agenten herzustellen, müssen Sie SSH verwenden. Stellen Sie sicher, dass die Sicherheitsgruppe Ihrer EC2 Instance den Zugriff mit SSH (TCP-Port 22) zulässt.

Führen Sie in einem Terminal den folgenden `ssh` Befehl aus, um eine Verbindung mit der Instanz herzustellen:

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Geben Sie für */path/key-pair-name* den Pfad und den Dateinamen (*.pem*) des privaten Schlüssels an, der für die Verbindung mit Ihrer Instance erforderlich ist.

- Legen Sie für *instance-user-name* die Option `admin` fest.
- Geben Sie für *instance-public-ip-address* die öffentliche IP-Adresse Ihrer Instance an.

Was bedeutet der Fehler Fehler beim Abrufen des Agenten-Aktivierungsschlüssels?

Bei der Aktivierung Ihres DataSync Agenten stellt der Agent eine Verbindung zu dem von Ihnen angegebenen Service-Endpunkt her, um einen Aktivierungsschlüssel anzufordern. Dieser Fehler bedeutet wahrscheinlich, dass Ihre Netzwerksicherheitseinstellungen die Verbindung blockieren.

Maßnahme

Wenn Sie einen Virtual Private Cloud (VPC) -Dienstendpunkt verwenden, stellen Sie sicher, dass Ihre Sicherheitsgruppeneinstellungen es Ihrem Agenten ermöglichen, eine Verbindung zum VPC-Endpunkt herzustellen. Informationen zu den erforderlichen Ports finden Sie unter [Netzwerkanforderungen für VPC- oder FIPS-VPC-Dienstendpunkte](#).

Wenn Sie einen öffentlichen Endpunkt oder einen FIPS-Endpunkt (Federal Information Processing Standard) verwenden, überprüfen Sie, ob Ihre Firewall- und Router-Einstellungen es Ihrem Agenten ermöglichen, eine Verbindung zum Endpunkt herzustellen. Weitere Informationen finden Sie unter [Netzwerkanforderungen für öffentliche Endpunkte oder FIPS-Dienstendpunkte](#).

Ich kann einen Agenten immer noch nicht mithilfe eines VPC-Dienstendpunkts aktivieren

Wenn Sie immer noch Probleme bei der Aktivierung eines DataSync Agenten mit einem VPC-Dienstendpunkt haben, finden Sie weitere Informationen unter [Ich weiß nicht, was mit meinem Agenten los ist. Kann mir jemand helfen?](#)

Was mache ich, wenn mein Agent offline ist?

Ihr DataSync Agent kann aus verschiedenen Gründen offline sein, aber Sie können ihn möglicherweise wieder online stellen. Bevor Sie den Agenten löschen und einen neuen erstellen, gehen Sie die folgende Checkliste durch, damit Sie verstehen, was möglicherweise passiert ist.

- Wenden Sie sich an Ihr Backup-Team — Wenn Ihr Agent offline ist, weil seine virtuelle Maschine (VM) aus einem Snapshot oder Backup wiederhergestellt wurde, müssen Sie [den Agenten möglicherweise ersetzen](#).

- Prüfen Sie, ob die VM oder EC2 Amazon-Instanz des Agenten ausgeschaltet ist — Versuchen Sie je nach Art des verwendeten Agenten, die VM oder EC2 Instanz wieder einzuschalten, falls sie ausgeschaltet ist. Sobald sie wieder eingeschaltet ist, [testen Sie die Netzwerkkonnektivität Ihres Agenten](#) mit AWS.
- Stellen Sie sicher, dass Ihr Agent die Mindestanforderungen an die Hardware erfüllt — Ihr Agent ist möglicherweise offline, weil seine VM- oder EC2 Instanzkonfiguration seit der Aktivierung des Agenten versehentlich geändert wurde. Wenn Ihre VM beispielsweise nicht mehr über den mindestens erforderlichen Arbeitsspeicher oder Speicherplatz verfügt, wird der Agent möglicherweise als offline angezeigt. Weitere Informationen finden Sie unter [Anforderungen für Agenten AWS DataSync](#).
- Warten Sie, bis die Agent-bezogenen Softwareupdates abgeschlossen sind — Ihr Agent wird möglicherweise kurzzeitig offline geschaltet, nachdem die [Softwareupdates von bereitgestellt wurden AWS](#). Wenn Sie glauben, dass der Agent aus diesem Grund offline ist, warten Sie einen kurzen Zeitraum und überprüfen Sie dann, ob der Agent wieder online ist.
- Überprüfen Sie Ihre VPC-Dienstendpunkteinstellungen — Wenn Ihr Offline-Agent einen öffentlichen Dienstendpunkt verwendet und sich auch in derselben VPC befindet, für die Sie einen VPC-Dienstendpunkt erstellt haben DataSync, müssen Sie möglicherweise die [private DNS-Unterstützung](#) für diesen VPC-Endpunkt deaktivieren.

[Wenn keiner dieser Gründe der Grund dafür zu sein scheint, dass der Agent offline ist, müssen Sie den Agenten wahrscheinlich ersetzen.](#)

Ich weiß nicht, was mit meinem Agenten los ist. Kann mir jemand helfen?

Sie können Ihrem DataSync Agenten AWS Support Zugriff gewähren und ihm bei der Behebung von Problemen mit dem Agenten helfen. Sie müssen diesen Zugriff über die lokale Konsole des Agenten aktivieren.

Um Ihrem Agenten Support Zugriff zu gewähren

1. [Melden Sie sich bei der lokalen Konsole Ihres Agenten](#) an.
2. Geben Sie an der Eingabeaufforderung die Eingabetaste ein, **5** um die Befehlszeile zu öffnen (für VMware VMs, verwenden**6**).
3. Geben Sie **h** ein, um das Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) zu öffnen.

4. Geben Sie im Fenster VERFÜGBARE BEFEHLE Folgendes ein, um eine Verbindung herzustellen Support:

open-support-channel

Wenn Sie den Agenten mit VPC-Endpunkten verwenden, müssen Sie wie folgt eine VPC-Endpunkt-IP-Adresse für Ihren Support-Kanal angeben:

open-support-channel *vpc-ip-address*

Ihre Firewall muss es dem eingehenden TCP-Port 22 ermöglichen, einen Support-Kanal zu initiieren. AWS Wenn Sie eine Verbindung zu herstellen Support, DataSync weist Ihnen eine Supportnummer zu. Notieren Sie sich Ihre Support-Nummer.

Note

Die Kanalnummer ist keine TCP/UDP Portnummer. Stattdessen stellt es eine SSH-Verbindung (TCP 22) zu Servern her und stellt den Supportkanal für die Verbindung bereit.

5. Wenn der Support-Kanal eingerichtet ist, geben Sie Ihre Support-Servicenummer an, Support damit dieser Ihnen bei der Fehlerbehebung helfen kann.
6. Wenn die Support-Sitzung beendet ist, drücken Sie, **Enter** um sie zu beenden.
7. Geben Sie ein **exit**, um sich von der DataSync lokalen Konsole abzumelden.
8. Folgen Sie den Eingabeaufforderungen, um die lokale Konsole zu beenden.

Behebung von Problemen mit DataSync Standorten

Verwenden Sie die folgenden Informationen, um Probleme mit AWS DataSync Standorten zu beheben. Zu diesen Problemen können gehören:

- Berechtigungen und Einhängfehler bei NFS-Speicherorten
- Probleme mit dem Besitz von Dateien
- Probleme beim Zugriff auf SMB-Standorte, die die Kerberos-Authentifizierung verwenden
- Berechtigungs- und Zugriffsprobleme mit Objektspeichern, z. B. Amazon S3- und Microsoft Azure Blob-Speicherorten

Meine Aufgabe ist mit der Fehlermeldung „NFS-Berechtigungen verweigert“ fehlgeschlagen

Sie können die Fehlermeldung „Berechtigungen verweigert“ erhalten, wenn Sie Ihren NFS-Dateiserver mit `root_squash` oder konfigurieren `all_squash` und Ihre Dateien nicht alle Lesezugriff haben.

Maßnahme

Um dieses Problem zu beheben, konfigurieren Sie Ihren NFS-Export mit `no_root_squash` oder stellen Sie sicher, dass die Berechtigungen für alle Dateien, die Sie übertragen möchten, allen Benutzern Lesezugriff gewähren.

DataSync Um auf Verzeichnisse zugreifen zu können, müssen Sie außerdem den All-Execute-Zugriff aktivieren. Um sicherzustellen, dass das Verzeichnis gemountet werden kann, verbinden Sie sich zunächst mit einem Computer, der die gleiche Netzwerkkonfiguration wie Ihr Agent hat. Führen Sie dann den folgenden CLI-Befehl aus:

```
mount -t nfs -o nfsvers=<your-nfs-server-version> <your-nfs-server-name>:<nfs-export-path-you-specified> <new-test-folder-on-your-computer>
```

Wenn das Problem immer noch nicht behoben ist, wenden Sie sich an [AWS Support das Center](#).

Meine Aufgabe ist mit einem NFS-Mount-Fehler fehlgeschlagen

Möglicherweise wird der folgende Fehler angezeigt, wenn Sie eine DataSync Aufgabe ausführen, die einen NFS-Dateiserverstandort beinhaltet:

Die Aufgabe konnte nicht auf den Speicherort zugreifen loc-1111222233334444a: x40016: mount.nfs: Verbindungs-Timeout

Zu ergreifende Maßnahmen

Gehen Sie wie folgt vor, bis der Fehler behoben ist.

1. Stellen Sie sicher, dass der NFS-Dateiserver und der Export, die Sie an Ihrem DataSync Standort angeben, gültig sind. Wenn dies nicht der Fall ist, löschen Sie Ihren Standort und Ihre Aufgabe und erstellen Sie dann einen neuen Speicherort und eine neue Aufgabe, die einen gültigen NFS-Dateiserver verwenden, und exportieren Sie sie. Weitere Informationen finden Sie unter [Verwenden der DataSync-Konsole](#).

2. Überprüfen Sie Ihre Firewall-Konfiguration zwischen Ihrem Agenten und dem NFS-Dateiserver. Weitere Informationen finden Sie unter [Netzwerkanforderungen für lokalen, selbstverwalteten und anderen Cloud-Speicher](#).
3. Stellen Sie sicher, dass Ihr Agent auf den NFS-Dateiserver zugreifen kann, und mounten Sie den Export. Weitere Informationen finden Sie unter [Bereitstellung des DataSync Zugriffs auf NFS-Dateiserver](#).
4. Wenn der Fehler weiterhin angezeigt wird, öffnen Sie einen Support-Kanal mit Support. Weitere Informationen finden Sie unter [Ich weiß nicht, was mit meinem Agenten los ist. Kann mir jemand helfen?](#).

Meine Aufgabe ist mit einem Amazon EFS-Mount-Fehler fehlgeschlagen

Möglicherweise wird der folgende Fehler angezeigt, wenn Sie eine DataSync Aufgabe ausführen, die einen Amazon EFS-Standort betrifft:

Die Aufgabe konnte nicht auf den Standort zugreifen loc-1111222233334444a: x40016: Es konnte keine Verbindung zum EFS-Mount-Ziel mit IP hergestellt werden: 10.10.1.0.

Dies kann passieren, wenn der Bereitstellungspfad des Amazon EFS-Dateisystems, den Sie mit Ihrem Standort konfigurieren, aktualisiert oder gelöscht wird. DataSync ist sich dieser Änderungen im Dateisystem nicht bewusst.

Maßnahme

Löschen Sie Ihren Standort und Ihre Aufgabe und [erstellen Sie einen neuen Amazon EFS-Speicherort](#) mit dem neuen Bereitstellungspfad.

Der Dateibesitz wird bei der NFS-Übertragung nicht beibehalten

Nach der Übertragung stellen Sie möglicherweise fest, dass die Dateien an Ihrem DataSync Zielspeicherort einen anderen Benutzer IDs (UIDs) oder eine andere Gruppe IDs (GIDs) haben als dieselben Dateien an Ihrem Quellspeicherort. Beispielsweise könnten die Dateien an Ihrem Zielort die UID 6553499, oder nobody haben.

Dies kann passieren, wenn ein Dateisystem, das an Ihrer Übertragung beteiligt ist, die ID-Zuordnung von NFS Version 4 verwendet, eine Funktion, die DataSync nicht unterstützt wird.

Maßnahme

Sie haben mehrere Möglichkeiten, dieses Problem zu umgehen:

- Erstellen Sie einen neuen Speicherort für das Dateisystem, das NFS Version 3 anstelle von Version 4 verwendet.
- Deaktivieren Sie die ID-Zuordnung von NFS Version 4 auf dem Dateisystem.

Versuchen Sie die Übertragung erneut. Beide Optionen sollten das Problem lösen.

Meine Aufgabe kann nicht auf einen SMB-Standort zugreifen, der Kerberos verwendet

DataSync Fehler bei SMB-Standorten, die die [Kerberos-Authentifizierung](#) verwenden, hängen in der Regel mit Diskrepanzen zwischen Ihrem Standort und den Kerberos-Konfigurationen zusammen. Möglicherweise liegt auch ein Netzwerkproblem vor.

Auf den Standort konnte nicht zugegriffen werden

Der folgende Fehler weist darauf hin, dass möglicherweise Konfigurationsprobleme mit Ihrem SMB-Standort oder dem Kerberos-Setup vorliegen:

```
Task failed to access location
```

Überprüfen Sie Folgendes:

- Der SMB-Dateiserver, den Sie für Ihren Standort angeben, ist ein Domainname. Für Kerberos können Sie die IP-Adresse des Dateiservers nicht angeben.
- Der Kerberos-Prinzipal, den Sie für Ihren Standort angeben, entspricht dem Prinzipal, den Sie zum Erstellen der Kerberos-Schlüsseltabellendatei (Keytab) verwenden. Bei Prinzipalnamen wird Groß- und Kleinschreibung beachtet.
- Das zugeordnete Benutzerkennwort des Kerberos-Prinzips hat sich seit der Erstellung der Keytab-Datei nicht geändert. Wenn sich das Passwort ändert (aufgrund einer Passwortrotation oder aus einem anderen Grund), schlägt die Ausführung der Aufgabe möglicherweise mit dem folgenden Fehler fehl:

Die Aufgabe konnte nicht auf den Standort zugreifen loc-1111222233334444a: x40015: kinit:

Beim Abrufen der ersten Anmeldeinformationen ist die Vorauthentifizierung fehlgeschlagen

Der KDC-Bereich kann nicht kontaktiert werden

Der folgende Fehler weist auf ein Netzwerkproblem hin:

```
kinit: Cannot contact any KDC for realm 'MYDOMAIN.ORG' while getting initial credentials"
```

Überprüfen Sie Folgendes:

- Die von Ihnen bereitgestellte Kerberos-Konfigurationsdatei (`krb5.conf`) DataSync enthält die richtigen Informationen zu Ihrem Kerberos-Bereich. [Eine `krb5.conf` Beispieldatei finden Sie unter Voraussetzungen für die Kerberos-Authentifizierung.](#)
- Der Kerberos Key Distribution Center (KDC) -Serverport ist geöffnet. Der KDC-Port ist in der Regel der TCP-Port 88.
- Die DNS-Konfiguration in Ihrem Netzwerk.

Meine Aufgabe ist mit einem input/output Fehler fehlgeschlagen

Sie können eine input/output Fehlermeldung erhalten, wenn Ihr Speichersystem die I/O Anforderungen des DataSync Agenten nicht erfüllt. Zu den häufigsten Gründen hierfür gehören ein Serverfestplattenausfall, Änderungen an Ihrer Firewall-Konfiguration oder ein Ausfall des Netzwerk-Routers.

Wenn der Fehler einen NFS-Dateiserver oder einen Hadoop Distributed File System (HDFS) -Cluster betrifft, gehen Sie wie folgt vor, um den Fehler zu beheben.

Zu ergreifende Maßnahmen (NFS)

Überprüfen Sie zunächst die Protokolle und Messwerte Ihres NFS-Dateiservers, um festzustellen, ob das Problem auf dem NFS-Server aufgetreten ist. Falls ja, lösen Sie das Problem.

Als nächstes überprüfen Sie, ob Ihre Netzwerkkonfiguration unverändert ist. Gehen Sie wie folgt vor, um zu überprüfen, ob der NFS-Dateiserver korrekt konfiguriert ist und darauf zugreifen DataSync kann:

1. Richten Sie einen anderen NFS-Client im gleichen Netzwerk-Subnetz wie den -Agenten ein.
2. Mounten Sie Ihre Freigabe auf diesem Client.
3. Überprüfen Sie, ob der Client die Freigabe erfolgreich lesen und schreiben kann.

Zu ergreifende Maßnahmen (HDFS)

Gehen Sie wie folgt vor, bis Sie den Fehler behoben haben:

1. Stellen Sie sicher, dass Ihr HDFS-Cluster Ihrem DataSync Agenten die Kommunikation mit den Clustern NameNode und DataNode Anschlüssen ermöglicht.

In den meisten Clustern finden Sie die Portnummern, die der Cluster verwendet, in den folgenden Konfigurationsdateien:

- Um den NameNode Port zu finden, suchen Sie in der `core-site.xml` Datei unter der `fs.default.name` Eigenschaft `fs.default` oder (abhängig von der Hadoop-Distribution).
 - Um den DataNode Port zu finden, suchen Sie in der `hdfs-site.xml` Datei unter der `dfs.datanode.address` Eigenschaft.
2. Vergewissern Sie sich in Ihrer `hdfs-site.xml` Datei, dass Ihre `dfs.data.transfer.protection` Eigenschaft nur einen Wert hat. Beispiel:

```
<property>
  <name>dfs.data.transfer.protection</name>
  <value>privacy</value>
</property>
```

Fehler: **FsS3UnableToConnectToEndpoint**

DataSync kann keine Verbindung zu Ihrem [Amazon S3 S3-Standort](#) herstellen. Dies kann bedeuten, dass der S3-Bucket des Standorts nicht erreichbar ist oder der Standort nicht richtig konfiguriert ist.

Gehen Sie wie folgt vor, bis Sie das Problem behoben haben:

- Prüfen Sie, ob DataSync Sie [auf Ihren S3-Bucket zugreifen](#) können.
- Stellen Sie mithilfe der DataSync Konsole oder des [DescribeLocationS3-Betriebs](#) sicher, dass der Standort korrekt konfiguriert ist.

Fehler: **FsS3HeadBucketFailed**

DataSync kann nicht auf den S3-Bucket zugreifen, zu dem oder von dem Sie übertragen. Prüfen Sie mithilfe des Amazon S3 [HeadBucket](#) S3-Vorgangs, ob DataSync Sie berechtigt sind, auf den Bucket zuzugreifen. Wenn Sie Ihre Berechtigungen anpassen müssen, finden Sie weitere Informationen unter [Bereitstellung des DataSync Zugriffs auf S3-Buckets](#).

Die Aufgabe schlägt mit einem **Unable to list Azure Blobs on the volume root** Fehler fehl

Wenn Ihre DataSync Übertragungsaufgabe mit einem `Unable to list Azure Blobs on the volume root` Fehler fehlschlägt, liegt möglicherweise ein Problem mit Ihrem SAS-Token (Shared Access Signature) oder dem Netzwerk Ihres Azure Speicherkontos vor.

Zu ergreifende Maßnahmen

Versuchen Sie Folgendes und führen Sie Ihre Aufgabe erneut aus, bis Sie das Problem behoben haben:

- Stellen Sie sicher, dass Ihr [SAS-Token](#) über die richtigen Berechtigungen für den Zugriff auf Ihr verfügtMicrosoft Azure Blob Storage.
- Wenn Sie Ihren DataSync Agenten in ausführenAzure, konfigurieren Sie Ihr Speicherkonto so, dass der Zugriff von dem virtuellen Netzwerk aus möglich ist, in dem sich Ihr Agent befindet.
- Wenn Sie Ihren Agenten auf Amazon ausführen EC2, konfigurieren Sie Ihre Azure Storage-Firewall so, dass der Zugriff von der öffentlichen IP-Adresse des Agenten aus möglich ist.

Informationen zur Konfiguration des Netzwerks Ihres Azure Speicherkontos finden Sie in der [Azure Blob StorageDokumentation](#).

Fehler: **FsAzureBlobVolRootListBlobsFailed**

Das SAS-Token (Shared Access Signature), das für den Zugriff auf Ihr DataSync verwendet wird, Microsoft Azure Blob Storage verfügt nicht über die Listenberechtigung.

Um das Problem zu beheben, [aktualisieren Sie Ihren Standort](#) mit einem Token, das über die Listenberechtigung verfügt, und versuchen Sie erneut, Ihre Aufgabe auszuführen.

Fehler: **SrcLocHitAccess**

DataSync kann nicht auf Ihren Quellstandort zugreifen. Vergewissern Sie DataSync sich, dass die Person berechtigt ist, auf den Speicherort zuzugreifen, und versuchen Sie erneut, Ihre Aufgabe auszuführen.

Fehler: **SyncTaskErrorLocationNotAdded**

DataSync kann nicht auf Ihren Standort zugreifen. Vergewissern Sie DataSync sich, dass die Person berechtigt ist, auf den Standort zuzugreifen, und versuchen Sie erneut, Ihre Aufgabe auszuführen.

Fehler: **S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation**

Dieser Fehler könnte mit IAM-Berechtigungen, Amazon S3 S3-Bucket-Richtlinien, AWS KMS Berechtigungen oder anderen Berechtigungsproblemen zusammenhängen. Wenn Sie diesen Fehler erhalten, verwenden Sie die folgenden Informationen zur Fehlerbehebung:

- [Beheben Sie Fehler mit Zugriff verweigert \(403 Forbidden\) in Amazon S3](#) im Amazon Simple Storage Service-Benutzerhandbuch
- [Wie behebe ich 403 Access Denied-Fehler von Amazon S3?](#) nein AWS re:Post

Die Aufgabe mit dem S3-Quellspeicherort schlägt mit **HeadObject** oder mit einem **GetObjectTagging** Fehler fehl

Fehler im Zusammenhang mit **HeadObject** oder **GetObjectTagging**

Wenn Sie Objekte mit einer bestimmten Version IDs aus einem S3-Bucket übertragen, wird möglicherweise ein Fehler im Zusammenhang mit **HeadObject** oder **getObjectTagging** angezeigt. Hier ist zum Beispiel ein Fehler im Zusammenhang mit **GetObjectTagging**:

```
[WARN] Failed to read metadata for file /picture1.png (versionId: 111111): S3 Get
Object Tagging Failed
[ERROR] S3 Exception: op=GetObjectTagging photos/picture1.png, code=403, type=15,
exception=AccessDenied,
msg=Access Denied req-hdrs: content-type=application/xml, x-amz-api-version=2006-03-01
rsp-hdrs: content-type=application/xml,
date=Wed, 07 Feb 2024 20:16:14 GMT, server=AmazonS3, transfer-encoding=chunked,
x-amz-id-2=IOWQ4fDEXAMPLEQM+ey7N9WgVhSnQ6JEXAMPLEZb7hSQDASK+Jd1vEXAMPLEa3Km, x-amz-
request-id=79104EXAMPLEB723
```

Wenn Sie einen dieser Fehler sehen, überprüfen Sie, ob die IAM-Rolle, die für den Zugriff auf Ihren S3-Quellspeicherort DataSync verwendet wird, über die folgenden Berechtigungen verfügt:

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

Informationen dazu, wie Sie Ihre Rolle mit diesen Berechtigungen aktualisieren müssen, finden Sie unter [Erstellen einer IAM-Rolle für den Zugriff DataSync auf Ihren Amazon S3 S3-Standort](#).

Behebung von Problemen mit DataSync Aufgaben

Verwenden Sie die folgenden Informationen, um Probleme mit AWS DataSync Aufgaben und Aufgabenausführungen zu beheben. Zu diesen Problemen können Probleme beim Einrichten von Aufgaben, hängengebliebene Aufgabenausführungen und nicht erwartungsgemäß übertragene Daten gehören.

Fehler: Ungültiger SyncOption Wert. Option: TransferModePreserveDeletedFiles, Wert: ALL, REMOVE.

Dieser Fehler tritt auf, wenn Sie Ihre DataSync Aufgabe erstellen oder bearbeiten und die Option Alle Daten übertragen auswählen und die Option Gelöschte Dateien behalten deaktivieren.

Wenn Sie alle Daten übertragen, wird Ihr Zielort DataSync nicht gescannt und Sie wissen nicht, was Sie löschen sollen.

Die Ausführung der Aufgabe schlägt mit einem `EniNotFound` Fehler fehl

Dieser Fehler tritt auf, wenn Sie eine der Netzwerkschnittstellen Ihrer Aufgabe in Ihrer Virtual Private Cloud (VPC) löschen. Wenn Ihre Aufgabe geplant ist oder sich in der Warteschlange befindet, schlägt die Aufgabe fehl, wenn eine [Netzwerkschnittstelle fehlt, die für die Übertragung Ihrer Daten erforderlich](#) ist.

Zu ergreifende Maßnahmen

Sie haben die folgenden Optionen, um dieses Problem zu umgehen:

- Starten Sie die Aufgabe manuell neu. Wenn Sie dies tun, DataSync werden alle fehlenden Netzwerkschnittstellen erstellt, die für die Ausführung der Aufgabe erforderlich sind.

- Wenn Sie Ressourcen in Ihrer VPC bereinigen müssen, stellen Sie sicher, dass Sie keine Netzwerkschnittstellen löschen, die sich auf eine DataSync Aufgabe beziehen, die Sie noch verwenden.

Gehen Sie wie folgt vor, um die Ihrer Aufgabe zugewiesenen Netzwerkschnittstellen zu sehen:

- Verwenden Sie die [DescribeTask](#) Operation. Sie können die Netzwerkschnittstellen in den Elementen `SourceNetworkInterfaceArns` und `DestinationNetworkInterfaceArns` Antwort anzeigen.
- Suchen Sie in der EC2 Amazon-Konsole nach Ihrer Aufgaben-ID (z. B. `task-f012345678abcdef0`), um deren Netzwerkschnittstellen zu finden.
- Erwägen Sie, Ihre Aufgaben nicht automatisch auszuführen. Dies könnte das Deaktivieren der Aufgabenwarteschlange oder der Zeitplanung (durch DataSync oder durch benutzerdefinierte Automatisierung) beinhalten.

Die Ausführung der Aufgabe schlägt fehl und es wird der Fehler „Speicher kann nicht zugewiesen werden“ angezeigt

Wenn Ihre DataSync Aufgabe mit dem Fehler „Speicher kann nicht zugewiesen werden“ fehlschlägt, kann das verschiedene Ursachen haben.

Maßnahme

Versuchen Sie Folgendes, bis das Problem nicht mehr auftritt:

- Wenn an Ihrer Übertragung ein Agent beteiligt ist, stellen Sie sicher, dass der Agent die Anforderungen für [virtuelle Maschinen \(VM\)](#) oder [EC2 Amazon-Instances](#) erfüllt.
- Teilen Sie Ihre Übertragung mithilfe von [Filtern](#) in mehrere Aufgaben auf. Es ist möglich, dass Sie versuchen, mehr Dateien oder Objekte zu übertragen, als [eine DataSync Aufgabe bewältigen kann](#).
- Wenn das Problem weiterhin auftritt, [wenden Sie sich an Support](#).

Die Aufgabe schlägt mit oder **Input/Output error** FSx für das ONTAP-Dateisystem fehl

Wenn Ihre DataSync Aufgabe bei einem `Input/Output error` beim Übertragen von Daten mit einem FSx für ONTAP Dateisystem fehlschlägt, kann dies an einem oder mehreren der folgenden Probleme liegen.

Das Volume FSx for ONTAP hat seine maximale Dateikapazität erreicht

Dieser Fehler tritt auf, wenn die Anzahl der verfügbaren Inodes oder Dateizeiger auf einem Volume erschöpft ist.

Zu ergreifende Maßnahmen

Sehen Sie sich zunächst die [maximale Dateikapazität](#) des Volumes an. Erhöhen Sie anschließend die Dateikapazität des Volumes, indem Sie entweder die Anzahl der Inodes oder die Speicherkapazität erhöhen. Weitere Informationen finden Sie unter [Erhöhen der maximalen Dateikapazität eines Volumes](#) im FSx for ONTAP-Benutzerhandbuch.

Die verfügbare Speicherkapazität des Volumes FSx für ONTAP ist aufgebraucht

Dieser Fehler tritt auf, wenn für das Volume keine verfügbare Speicherkapazität verfügbar ist.

Zu ergreifende Maßnahmen

Ermitteln Sie zunächst die [verfügbare Speicherkapazität](#) des Volumes. Erhöhen Sie anschließend die Speicherkapazität des Volumes. Weitere Informationen finden Sie unter [Erhöhen der Speicherkapazität eines Volumes](#) im FSx for ONTAP-Benutzerhandbuch.

 Note

Informationen zur automatischen Erhöhung der Speicherkapazität eines Volumes bei Bedarf finden Sie unter [Verwenden der automatischen Volumengrößenanpassung](#) im FSx for ONTAP-Benutzerhandbuch.

Das Verzeichnis FSx for ONTAP hat die maximale Anzahl von Dateien erreicht, die in jedem Verzeichnis gespeichert werden können

Dieser Fehler tritt auf, wenn Sie die maximale Anzahl von Dateien erreicht haben, die in jedem Verzeichnis gespeichert werden können.

Maßnahme

Erhöhen Sie die maximale Verzeichnisgröße, um größere Verzeichnisse zu unterstützen. Weitere Informationen finden Sie unter [Bewährte Methoden für die Verwendung der maximalen Verzeichnisgröße FSx für ONTAP](#) in AWS Prescriptive Guidance.

Bei der Ausführung der DataSync Aufgabe wurde zu viel Parallelität beim Lesen und Schreiben erzeugt, wodurch ein Großteil der Durchsatzkapazität des Dateisystems beansprucht wurde

Dieser Fehler tritt auf, wenn die Ausführung der DataSync Aufgabe zu viel von der verfügbaren Durchsatzkapazität Ihres Dateisystems beansprucht.

Zu ergreifende Maßnahmen

Stellen Sie zunächst mithilfe der folgenden Methoden fest, ob die Ausführung der Aufgabe zu viel von der Durchsatzkapazität des Dateisystems beansprucht hat:

- Überwachen Sie die Leistung des Dateisystems anhand der verfügbaren CloudWatch Messwerte. Weitere Informationen finden Sie unter [Überwachung von Dateisystem-Metriken](#) im FSx for ONTAP User Guide.
- Überwachen Sie das Dateisystem in der FSx Amazon-Konsole auf Leistungswarnungen des Dateiservers. Weitere Informationen finden Sie unter [Leistungswarnungen und Empfehlungen](#) im FSx ONTAP-Benutzerhandbuch.

Stellen Sie anschließend sicher, dass die Aufgabe nicht die gesamte verfügbare Durchsatzkapazität des Dateisystems nutzt, indem Sie einen der folgenden Schritte ausführen:

- Legen Sie das Bandbreitenlimit für die Ausführung der Aufgabe auf einen Wert fest, der unter der FSx für das ONTAP-Dateisystem bereitgestellten Durchsatzkapazität liegt. Weitere Informationen finden Sie unter [Legen Sie Bandbreitenlimits für Ihre Aufgabe fest AWS DataSync](#).
- Erhöhen Sie die bereitgestellte Durchsatzkapazität des Dateisystems. Weitere Informationen finden Sie unter [Aktualisierung der Durchsatzkapazität](#) im Benutzerhandbuch FSx für ONTAP.

Die Aufgabe schlägt fehl mit **Connection Reset by peer** oder **Host is down** Meldung FSx für das ONTAP-Dateisystem

Wenn Ihre DataSync Aufgabe bei der Übertragung von Daten mit einem Dateisystem FSx für ONTAP mit der Host is down Meldung Connection Reset by peer oder fehlschlägt, kann dies an einem oder mehreren der folgenden Probleme liegen:

- Der SMB-Server des Dateisystems wurde während der Ausführung der Aufgabe neu gestartet oder auf andere Weise unterbrochen.

- Das Dateisystem führte während der Ausführung der Aufgabe einen Failover vom primären zum sekundären Server (und zur IP-Adresse) durch. DataSync unterstützt kein Failover auf eine sekundäre IP-Adresse während der Ausführung der Aufgabe.

FSx für ONTAP-Dateisysteme erfolgt bei folgenden Ereignissen ein Failover auf einen sekundären Server und eine sekundäre IP-Adresse:

- Der Primärserver ist nicht mehr verfügbar.
- Die Availability Zone des Primärservers ist nicht mehr verfügbar (für Multi-AZ-Dateisysteme).
- Während einer vom Benutzer initiierten Änderung der Durchsatzkapazität.
- Während des regelmäßig geplanten Wartungsfensters des Dateisystems.

Weitere Informationen finden Sie unter [FSx ONTAP Failover Process](#) im FSx for ONTAP User Guide.

Maßnahme

Starten Sie die Aufgabe neu.

Die Ausführung der Aufgabe hat einen Startstatus, aber es scheint nichts zu passieren

Ihre DataSync Aufgabe kann in der Regel mit dem Status Wird gestartet hängen bleiben, weil der Agent ausgeschaltet ist oder die Netzwerkverbindung unterbrochen wurde.

Zu ergreifende Maßnahmen

Vergewissern Sie sich, dass der Status Ihres Agenten ONLINE ist. Wenn der Agent OFFLINE ist, stellen Sie sicher, dass er eingeschaltet ist.

Wenn der Agent eingeschaltet ist und die Aufgabe immer noch gestartet wird, liegt wahrscheinlich ein Netzwerkverbindungsproblem zwischen Ihrem Agenten und vor AWS. Weitere Informationen zum Testen der Netzwerkverbindung finden Sie unter [Überprüfen Sie die Verbindung Ihres Agenten mit dem Dienst DataSync](#).

Falls dieses Problem weiterhin besteht, finden Sie weitere Informationen unter [Ich weiß nicht, was mit meinem Agenten los ist. Kann mir jemand helfen?](#).

Die Aufgabenausführung scheint im Vorbereitungsstatus stecken geblieben zu sein

Wie lange Ihre DataSync Übertragungsaufgabe den Status In Vorbereitung hat, hängt von der Datenmenge in Ihrer Übertragungsquelle und Ihrem Übertragungsziel sowie von der Leistung dieser Speichersysteme ab.

Wenn eine Aufgabe gestartet wird, DataSync führt sie eine rekursive Verzeichnisliste durch, um alle Dateien, Objekte, Verzeichnisse und Metadaten in Ihrer Quelle und Ihrem Ziel zu ermitteln. DataSync verwendet diese Auflistungen, um Unterschiede zwischen Speichersystemen zu identifizieren und zu bestimmen, was kopiert werden soll. Dieser Vorgang kann einige Minuten oder sogar einige Stunden dauern.

Maßnahme

Du solltest nichts tun müssen. Warten Sie weiter, bis sich der Aufgabenstatus auf Wird übertragen ändert. Wenn sich der Status immer noch nicht ändert, wenden Sie sich an [AWS Support das Center](#).

Die Ausführung der Aufgabe wird beendet, bevor die Übertragung abgeschlossen ist

Wenn Ihre DataSync Aufgabenausführung vorzeitig beendet wird, enthält Ihre Aufgabenkonfiguration möglicherweise eine AWS-Region , die in Ihrem deaktiviert ist AWS-Konto.

Zu ergreifende Maßnahmen

Gehen Sie wie folgt vor, um Ihre Aufgabe erneut auszuführen:

1. Prüfen Sie den [Opt-In-Status](#) der Regionen Ihrer Aufgabe und stellen Sie sicher, dass sie aktiviert sind.
2. [Starte die Aufgabe](#) erneut.

Die Ausführung der Aufgabe schlägt fehl, wenn sie aus einem Google Cloud Storage-Bucket übertragen wird

Da DataSync die Kommunikation mit Google Cloud Storage über die Amazon S3 S3-API erfolgt, gibt es eine Einschränkung, die dazu führen kann, dass Ihre DataSync Übertragung fehlschlägt,

wenn Sie versuchen, Objekt-Tags zu kopieren. Die folgende Meldung zu dem Problem wird in Ihren CloudWatch Protokollen angezeigt:

[WARN] Fehler beim Lesen der Metadaten für die Datei/*your-bucket/your-object*: S3 Get Object Tagging Failed: Fortfahren ohne Tagging

Um dies zu verhindern, deaktivieren Sie bei der Konfiguration der Einstellungen für die Übertragungsaufgabe die Option Objekt-Tags kopieren.

Es gibt Diskrepanzen zwischen den Zeitstempeln der Aufgabenausführung

Wenn Sie sich die DataSync Konsole oder die CloudWatch Amazon-Protokolle ansehen, stellen Sie möglicherweise fest, dass die Start- und Endzeiten für die Ausführung Ihrer DataSync Aufgabe nicht mit den Zeitstempeln übereinstimmen, die Sie in anderen Überwachungstools sehen. [Das liegt daran, dass die Konsole und die CloudWatch Protokolle die Zeit berücksichtigen, die eine Aufgabenausführung im Startmodus oder in der Warteschlange verbringt, während dies bei einigen anderen Tools nicht der Fall ist.](#)

Möglicherweise stellen Sie diese Diskrepanz fest, wenn Sie die Ausführungszeitstempel zwischen der DataSync Konsole oder den CloudWatch Protokollen und den folgenden Stellen vergleichen:

- Protokolle für das Dateisystem, das an Ihrer Übertragung beteiligt ist
- Das Datum der letzten Änderung an einem Amazon S3 S3-Objekt, in das DataSync geschrieben wurde
- Netzwerkverkehr, der vom DataSync Agenten kommt
- EventBridge Amazon-Veranstaltungen

Die Ausführung der Aufgabe schlägt mit einem **NoMem** Fehler fehl

Der Datensatz, für den Sie übertragen möchten, ist möglicherweise zu groß DataSync. Wenn Sie diesen Fehler sehen, wenden Sie sich an des [AWS Support -Center](#).

Die Ausführung der Aufgabe schlägt mit einem **FsNfsIdMappingEnabled** Fehler fehl

DataSync unterstützt keine NFSv4 ID-Zuordnung. Um dieses Problem zu umgehen, [konfigurieren Sie den zu NFSv3 verwendenden NFS-Standort](#).

Das Objekt kann nicht übertragen werden (Fehler) Azure Blob Storage **user metadata key**

Bei der Übertragung von einem S3-Bucket zu Azure Blob Storage wird möglicherweise der folgende Fehler angezeigt:

```
[ERROR] Failed to transfer file /user-metadata/file1: Azure Blob user metadata key must be a CSharp identifier
```

Dies bedeutet, dass Benutzermetadaten */user-metadata/file1* enthalten sind, die keinen gültigen C#-Bezeichner verwenden. Weitere Informationen finden Sie in der [Microsoft-Dokumentation](#).

Am Zielort **/.aws-datasync** befindet sich ein Ordner

DataSync erstellt einen Ordner mit dem Namen **/.aws-datasync** an Ihrem Zielort, um Ihre Datenübertragung zu erleichtern.

Dieser Ordner wird DataSync normalerweise nach der Übertragung gelöscht, es kann jedoch Situationen geben, in denen dies nicht der Fall ist.

Maßnahme

Löschen Sie diesen Ordner jederzeit, solange Sie nicht gerade eine Aufgabe ausführen, die an diesen Speicherort kopiert.

Symbolische Links können mit SMB nicht zwischen Standorten übertragen werden

Wenn Ihre Aufgabenausführung abgeschlossen ist, wird der folgende Fehler angezeigt:

```
Transfer and verification completed. Selected files transferred except for files skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please contact AWS Support for further assistance.
```

Bei der Übertragung zwischen SMB-Speichersystemen (z. B. einem SMB-Dateiserver und dem Dateisystem Amazon FSx for Windows File Server) werden möglicherweise die folgenden Warnungen und Fehler in Ihren CloudWatch Protokollen angezeigt:

```
[WARN] Failed to read metadata for file /appraiser/symlink: No data available
[ERROR] Failed to read metadata for directory /appraiser/symlink: No data available
```

Maßnahme

DataSync unterstützt die Übertragung von symbolischen Links (oder Hardlinks) bei der Übertragung zwischen diesen Speicherorten nicht. Weitere Informationen finden Sie unter [Links und Verzeichnisse, die kopiert wurden von AWS DataSync](#).

Aufgabe: Fehler melden

Beim Versuch, Ihre DataSync Übertragung mit einem Aufgabenbericht zu überwachen, kann einer der folgenden Fehler auftreten.

Fehlermeldung	Workaround
Der Dateipfad überschreitet die maximale Länge von 4.096 Zeichen. In den Aufgabenbericht kann nicht geschrieben werden	Keiner. DataSync kann keine Datei mit einem Pfad übertragen, der 4.096 Byte überschreitet. Weitere Informationen finden Sie unter Speichersystem-, Datei- und Objektbeschränkungen .
Aufgabenbericht (e) konnten aufgrund eines ungültigen Buckets oder einer ungültigen IAM-Rolle nicht auf S3 hochgeladen werden	Vergewissern Sie sich, dass die DataSync IAM-Rolle über die richtigen Berechtigungen verfügt, um einen Aufgabenbericht in Ihren S3-Bucket hochzuladen.
Vor dem Generieren von Task-Berichten ist ein Ausführungsfehler aufgetreten	Überprüfen Sie Ihre CloudWatch Protokolle , um herauszufinden, warum die Ausführung Ihrer Aufgabe fehlgeschlagen ist.

Behebung von Problemen mit der Datenüberprüfung

AWS DataSync [Überprüft standardmäßig die Integrität](#) Ihrer Daten am Ende einer Übertragung. Verwenden Sie die folgenden Informationen, um häufig auftretende Fehler und Warnungen bei der Überprüfung zu diagnostizieren, z. B. wenn Dateien geändert oder gelöscht werden, bevor die Überprüfung Ihrer Daten DataSync abgeschlossen ist.

Bei Problemen mit der Überprüfung ist es oft hilfreich, zusätzlich zu dem angezeigten Fehler bei der [Aufgabenausführung auch Ihre CloudWatch Protokolle \(oder Aufgabenberichte\)](#) zu überprüfen. DataSync stellt JSON-strukturierte Protokolle für Aufgaben im erweiterten Modus bereit, während Aufgaben im Basismodus unstrukturierte Protokolle enthalten.

Es gibt Diskrepanzen zwischen den Inhalten einer Datei

Wenn Ihre Aufgabenausführung abgeschlossen ist, wird der folgende Fehler angezeigt:

```
Transfer and verification completed. Verification detected mismatches. Files with mismatches are listed in Cloud Watch Logs
```

In Ihren CloudWatch Protokollen stellen Sie möglicherweise fest, dass bei der Überprüfung von Inhalten, die sich zwischen Quell- und Zielspeicherort unterscheiden, Fehler aufgetreten sind. Dies kann passieren, wenn Dateien während Ihrer Übertragung geändert werden.

Aus den folgenden Protokollen geht beispielsweise hervor, dass es unterschiedliche dstHash Werte für mtimesrcHash, und file1.txt hat:

Beispiel für ein Protokoll im Basismodus

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt  srcMeta: type=R mode=0755 uid=65534
gid=65534 size=534528 atime=1633100003/684349800 mtime=1602647222/222919600
extAttrsHash=0
[NOTICE]  srcHash: 0c506c26bd1e43bd3ac346734f1a9c16c4ad100d1b43c2903772ca894fd24e44
[NOTICE] /directory1/directory2/file1.txt  dstMeta: type=R mode=0755 uid=65534
gid=65534 size=511001 atime=1633100003/684349800 mtime=1633106855/859227500
extAttrsHash=0
[NOTICE]  dstHash: dbd798929f11a7c0201e97f7a61191a83b4e010a449dfc79fbb8233801067c46
```

In mtime steht für den Zeitpunkt DataSync, an dem vor der [Vorbereitung](#) zum letzten Mal in eine Datei geschrieben wurde. DataSync Vergleicht bei der Überprüfung von Übertragungen mtime Werte zwischen Quell- und Zielspeicherorten. Ein solcher Überprüfungsfehler tritt auf, wenn der mtime Wert für eine Datei nicht für beide Speicherorte identisch ist. Die Unterschiede zwischen srcHash und dstHash deuten darauf hin, dass der Inhalt der Datei nicht an beiden Speicherorten übereinstimmt.

Zu ergreifende Maßnahmen

Gehen Sie wie folgt vor:

1. Verwenden Sie einen Epochenzeitkonverter, um festzustellen, ob die Quell- oder Zieldatei oder das Objekt in jüngerer Zeit geändert wurde. Auf diese Weise können Sie ermitteln, welche Version aktuell ist.
2. Um diesen Fehler erneut zu vermeiden, sollten [Sie Ihre Aufgabe so planen](#), dass sie während eines Wartungsfensters ausgeführt wird, wenn an Ihrer Quelle und Ihrem Ziel keine Aktivität stattfindet.

Die SMB-Metadaten einer Datei stimmen nicht überein

Wenn Ihre Aufgabenausführung abgeschlossen ist, wird der folgende Fehler angezeigt:

```
Transfer and verification completed. Verification detected mismatches. Files with mismatches are listed in Cloud Watch Logs
```

Bei der Übertragung zwischen Speichersystemen, die das Server Message Block (SMB) -Protokoll unterstützen, wird dieser Fehler möglicherweise angezeigt, wenn die erweiterten SMB-Attribute einer Datei nicht zwischen Quelle und Ziel übereinstimmen.

Aus den folgenden Protokollen geht beispielsweise hervor, dass der `extAttrsHash` Wert zwischen den Speicherorten unterschiedlich `file1.txt` ist, was darauf hindeutet, dass der Dateiinhalt identisch ist, aber am Ziel keine erweiterten Attribute festgelegt wurden:

Beispiel für ein Protokoll im Basismodus

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt  srcMeta: type=R mode=0755 uid=65534
gid=65534 size=1469752 atime=1631354985/174924200 mtime=1536995541/986211400
extAttrsHash=2272191894
[NOTICE]  srcHash: 38571d42b646ac8f4034b7518636b37dd0899c6fc03cdaa8369be6e81a1a2bb5
[NOTICE] /directory1/directory2/file1.txt  dstMeta: type=R mode=0755 uid=65534
gid=65534 size=1469752 atime=1631354985/174924200 mtime=1536995541/986211400
extAttrsHash=3051150340
[NOTICE]  dstHash: 38571d42b646ac8f4034b7518636b37dd0899c6fc03cdaa8369be6e81a1a2bb5
```

Möglicherweise wird Ihnen auch eine entsprechende Fehlermeldung zu erweiterten Attributen angezeigt:

```
[ERROR] Deferred error: WriteFileExtAttr2 failed to setextattrlist(filename="/directory1/directory2/file1.txt"): Input/output error
```

Maßnahme

Dieser Fehler tritt normalerweise auf, wenn nicht genügend Berechtigungen zum Kopieren von Zugriffskontrolllisten (ACLs) an das Ziel vorhanden sind. Lesen Sie je nach Zieltyp die folgenden Konfigurationshandbücher, um dieses Problem zu beheben:

- [Erforderliche Berechtigungen](#) FSx für Windows File Server-Dateisysteme
- [Erforderliche Berechtigungen](#) FSx für ONTAP-Dateisysteme, die SMB verwenden

Die zu übertragenden Dateien befinden sich nicht mehr am Quellspeicherort

Wenn Ihre Aufgabenausführung abgeschlossen ist, wird der folgende Fehler angezeigt:

```
Transfer and verification completed. Selected files transferred except for files  
skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please  
contact AWS Support for further assistance.
```

In Ihren Protokollen werden möglicherweise Fehler angezeigt, die darauf hinweisen, dass sich die Dateien nicht am Quellspeicherort befinden. Dies kann passieren, wenn Dateien (wie `file1.dll` und `file2.dll`) nach der [Vorbereitung](#), aber vor der DataSync Übertragung gelöscht werden:

Beispiel für ein Protokoll im Basismodus

```
[ERROR] Failed to open source file /file1.dll: No such file or directory  
[ERROR] Failed to open source file /file2.dll: No such file or directory
```

Maßnahme

Um diese Situationen zu vermeiden, sollten [Sie Ihre Aufgabe so planen](#), dass sie ausgeführt wird, wenn am Quellspeicherort keine Aktivität stattfindet.

Sie können Ihre Aufgabe beispielsweise während eines Wartungsfensters ausführen, wenn Benutzer und Anwendungen nicht aktiv an diesem Standort arbeiten.

In einigen Fällen werden Ihnen möglicherweise keine Protokolle angezeigt, die mit diesem Fehler verknüpft sind. Wenden Sie sich in diesem Fall an [AWS Support das Center](#).

DataSync kann die Zieldaten nicht verifizieren

Wenn Ihre Aufgabenausführung abgeschlossen ist, wird der folgende Fehler angezeigt:

Transfer and verification completed. Verification detected mismatches. Files with mismatches are listed in Cloud Watch Logs

In Ihren Protokollen stellen Sie möglicherweise fest, dass bestimmte Ordner oder Dateien am Zielort nicht verifiziert werden DataSync können. Diese Fehler können wie folgt aussehen:

Beispiel für ein Protokoll im Basismodus

```
[ERROR] Failed to read metadata for destination file /directory1/directory2/
file1.txt: No such file or directory
```

Bei Dateien treten möglicherweise Bestätigungsfehler wie folgt auf:

Beispiel für ein Protokoll im Basismodus

[illegible]

Maßnahme

Diese Protokolle weisen darauf hin, dass die Zieldaten nach der Übertragung, aber vor der Überprüfung gelöscht wurden. (Protokolle sehen ähnlich aus, wenn Daten im selben Zeitraum an einen Quellspeicherort hochgeladen werden.)

Um diese Situationen zu vermeiden, sollten Sie Ihre Aufgabe so planen, dass sie ausgeführt wird, wenn am Zielort keine Aktivität stattfindet.

Sie können Ihre Aufgabe beispielsweise während eines Wartungsfensters ausführen, wenn Benutzer und Anwendungen nicht aktiv an diesem Standort arbeiten.

DataSync kann Objektmetadaten nicht lesen

Wenn Ihre Aufgabenausführung abgeschlossen ist, wird der folgende Fehler angezeigt:

```
Transfer and verification completed. Selected files transferred except for files
skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please
contact AWS Support for further assistance.
```

In Ihren Protokollen stellen Sie möglicherweise fest, dass `file1.png` aufgrund einer fehlgeschlagenen Amazon S3 HeadObject S3-Anfrage nicht gelesen werden kann. [DataSync stellt während der Vorbereitung und Überprüfung von Aufgaben HeadObject Anfragen an S3-Standorte.](#)

Beispiel für ein Protokoll im Basismodus

```
[WARN] Failed to read metadata for file /file1.png: S3 Head Object Failed
```

Zu ergreifende Maßnahmen

Um dieses Problem zu beheben, überprüfen Sie, ob Sie DataSync über die richtigen Berechtigungen verfügen, um mit Ihrem S3-Bucket zu arbeiten:

- Stellen Sie sicher, dass die IAM-Rolle, die für den Zugriff auf Ihre Amazon S3 S3-Standorte DataSync verwendet wird, die `s3:GetObject` Genehmigung erteilt. Weitere Informationen finden Sie unter [Erforderliche Berechtigungen](#).
- Wenn Ihr S3-Bucket serverseitige Verschlüsselung verwendet, stellen Sie sicher, DataSync dass er auf die Objekte in diesem Bucket zugreifen darf. Weitere Informationen finden Sie unter [Zugriff auf S3-Buckets mithilfe serverseitiger Verschlüsselung](#).

Die systemdefinierten Metadaten eines Objekts stimmen nicht überein

Wenn Ihre Aufgabenausführung im erweiterten Modus zwischen S3-Buckets abgeschlossen ist, wird der folgende Fehler angezeigt:

```
Verification failed due to a difference in metadata
```

Möglicherweise stellen Sie in Ihren Protokollen fest, dass die [systemdefinierten Amazon S3 S3-Metadaten](#) eines Objekts nicht übereinstimmen. In diesem speziellen Beispiel hat das Quellobjekt

keine Content-Type Metadaten, das Zielobjekt jedoch. Dies geschah, weil der Ziel-S3-Bucket automatisch "ContentType": "application/octet-stream" Metadaten auf das Objekt angewendet hat, als es dorthin DataSync übertragen wurde.

Beispiel für ein Protokoll im erweiterten Modus

```
{
  "Action": "VERIFY",
  "Source": {
    "LocationId": "loc-0b3017fc4ba4a2d8d",
    "RelativePath": "encoding/content-null",
    "Metadata": {
      "Type": "Object",
      "ContentSize": 24,
      "LastModified": "2024-12-23T15:48:15Z",
      "S3": {
        "SystemMetadata": {
          "ETag": "\"68b9c323bb846841ee491481f576ed4a\""
        },
        "UserMetadata": {},
        "Tags": {}
      }
    }
  },
  "Destination": {
    "LocationId": "loc-abcdef01234567890",
    "RelativePath": "encoding/content-null",
    "Metadata": {
      "Type": "Object",
      "ContentSize": 24,
      "LastModified": "2024-12-23T16:00:03Z",
      "S3": {
        "SystemMetadata": {
          "ContentType": "application/octet-stream",
          "ETag": "\"68b9c323bb846841ee491481f576ed4a\""
        },
        "UserMetadata": {
          "file-mtime": "1734968895000"
        },
        "Tags": {}
      }
    }
  }
},
```

```
"TransferType": "CONTENT_AND_METADATA",  
"ErrorCode": "MetadataDiffers",  
"ErrorDetail": "Verification failed due to a difference in metadata"  
}
```

Maßnahme

Um diesen Fehler zu vermeiden, aktualisieren Sie Ihre Quellstandortobjekte so, dass sie die Content-Type Metadaten-Eigenschaft enthalten.

Grundlegendes zur Dauer der Datenüberprüfung

DataSync Die Überprüfung umfasst eine SHA256 Prüfsumme für den Dateiinhalt und einen genauen Vergleich der Dateimetadaten zwischen Speicherorten. Wie lange die Überprüfung dauert, hängt von mehreren Faktoren ab, darunter der Anzahl der beteiligten Dateien oder Objekte, der Größe der Daten in den Speichersystemen und der Leistung dieser Systeme.

Maßnahme

Angesichts der Faktoren, die sich auf die Dauer der Überprüfung auswirken können, sollten Sie nichts weiter tun müssen. Wenn bei der Ausführung Ihrer Aufgabe jedoch der Status „[Verifizierung](#)“ festgefahren zu sein scheint, wenden Sie sich an das [AWS Support Center](#).

Fehlerbehebung bei höheren als erwarteten S3-Speicherkosten mit DataSync

Wenn Ihre Amazon S3 S3-Speicherkosten nach einer AWS DataSync Übertragung höher sind, als Sie dachten, kann das an einem oder mehreren der folgenden Gründe liegen:

- Bei der Übertragung zu oder aus S3-Buckets entstehen Ihnen Kosten im Zusammenhang mit S3-API-Anfragen von DataSync
- DataSync verwendet die mehrteilige Upload-Funktion von Amazon S3, um Objekte in S3-Buckets hochzuladen. Dieser Ansatz kann zu unerwarteten Speichergebühren für Uploads führen, die nicht erfolgreich abgeschlossen werden.
- DataSync kopiert Objekt-Tags aus Quell- und Zielobjekten, wenn die Option Objekt-Tags kopieren in der Konsole aktiviert oder auf PRESERVE eingestellt ObjectTags ist. Beim Kopieren dieser Objekt-Tags können Kosten für S3-API-Anfragen anfallen.

- Die Objektversionierung kann für Ihr S3-Bucket aktiviert sein. Die Objektversionierung führt dazu, dass Amazon S3 mehrere Kopien von Objekten speichert, die denselben Namen haben.

Zu ergreifende Maßnahmen

In diesen Fällen können Sie die folgenden Schritte durchführen:

- Vergewissern Sie sich, dass Sie verstehen, wie S3-Anfragen DataSync verwendet werden und wie sich diese auf Ihre Speicherkosten auswirken könnten. Weitere Informationen finden Sie unter [Bewertung der Kosten für S3-Anfragen bei der Verwendung DataSync](#).
- Wenn das Problem mit mehrteiligen Uploads zusammenhängt, konfigurieren Sie eine Richtlinie für mehrteilige Uploads für Ihren S3-Bucket, um unvollständige mehrteilige Uploads zu bereinigen und so die Speicherkosten zu senken. Weitere Informationen finden Sie im AWS Blogbeitrag [S3 Lifecycle Management Update — Support for Multipart Uploads and Delete](#) Markers.
- Wenn das Problem mit dem Kopieren von Objekt-Tags zusammenhängt und Sie keine Objekt-Tags benötigen, deaktivieren Sie das Kontrollkästchen Objekt-Tags kopieren in der DataSync Konsole oder setzen Sie es ObjectTags auf, None wenn Sie eine Aufgabe erstellen, starten oder aktualisieren.
- Wenn das Problem mit der Objektversionierung zusammenhängt, deaktivieren Sie die Objektversionierung in Ihrem S3-Bucket.

[Wenn Sie weitere Hilfe benötigen, wenden Sie sich an AWS Support das Center.](#)

AWS DataSync Anleitungen

Diese Tutorials führen Sie durch einige reale Szenarien mit AWS DataSync

Themen

- [Tutorial: Übertragung von Daten vom lokalen Speicher zu Amazon S3 über AWS-Konten](#)
- [Tutorial: Daten zwischen Amazon S3 S3-Buckets übertragen AWS-Konten](#)

Tutorial: Übertragung von Daten vom lokalen Speicher zu Amazon S3 über AWS-Konten

Bei Verwendung AWS DataSync mit lokalem Speicher übertragen Sie in der Regel Daten an einen AWS Speicherdienst, der zu demselben gehört AWS-Konto wie Ihr DataSync Agent. Es gibt jedoch Situationen, in denen Sie möglicherweise Daten in einen Amazon S3 S3-Bucket übertragen müssen, der mit einem anderen Konto verknüpft ist.

Important

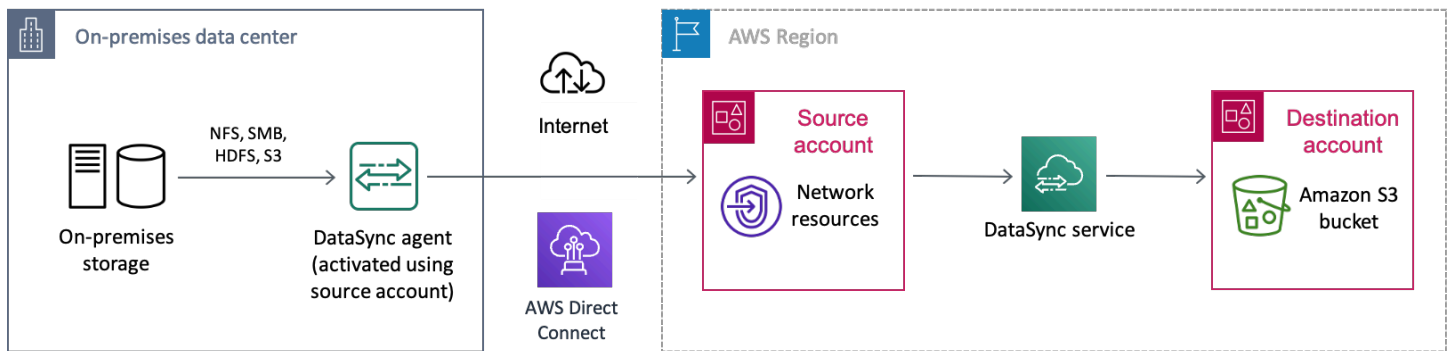
Die Übertragung AWS-Konten von Daten mithilfe der Methoden in diesem Tutorial funktioniert nur, wenn Amazon S3 einer der DataSync Übertragungsorte ist.

-Übersicht

Es ist nicht ungewöhnlich, dass Daten zwischen verschiedenen übertragen werden müssen AWS-Konten, insbesondere wenn Sie separate Teams haben, die die Ressourcen Ihres Unternehmens verwalten. So kann eine kontoübergreifende Übertragung DataSync mithilfe von:

- Quellkonto: Das AWS-Konto für die Verwaltung von Netzwerkressourcen. Dies ist das Konto, mit dem Sie Ihren DataSync Agenten aktivieren.
- Zielkonto: Das Konto AWS-Konto für die Verwaltung des S3-Buckets, in den Sie Daten übertragen müssen.

Das folgende Diagramm veranschaulicht ein solches Szenario.



Voraussetzung: Erforderliche Quellkontoberechtigungen

Für Ihre Quelle AWS-Konto sind bei dieser Art der kontoübergreifenden Übertragung zwei Arten von Berechtigungen zu berücksichtigen:

- Benutzerberechtigungen, mit denen ein Benutzer arbeiten kann DataSync (dies können Sie oder Ihr Speicheradministrator sein). Mit diesen Berechtigungen können Sie DataSync Standorte und Aufgaben erstellen.
- DataSync Serviceberechtigungen, die es DataSync ermöglichen, Daten in den Bucket Ihres Zielkontos zu übertragen.

User permissions

Fügen Sie in Ihrem Quellkonto mindestens die folgenden Berechtigungen zu einer IAM-Rolle hinzu, um Ihre DataSync Standorte und Aufgaben zu erstellen. Informationen zum Hinzufügen von Berechtigungen zu einer Rolle finden Sie unter Eine IAM-Rolle [erstellen](#) oder [ändern](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SourceUserRolePermissions",
      "Effect": "Allow",
      "Action": [
        "datasync:CreateLocationS3",
        "datasync:CreateTask",
        "datasync:DescribeLocation*",
        "datasync:DescribeTaskExecution",
        "datasync:ListLocations",
        "datasync:ListTaskExecutions",

```

```

        "datasync:DescribeTask",
        "datasync:CancelTaskExecution",
        "datasync:ListTasks",
        "datasync:StartTaskExecution",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
},
{
    "Sid": "IAMPermissions",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam:ListRoles",
        "iam:CreatePolicy"
    ],
    "Resource": "arn:aws:iam::111122223333:role/DataSync-*"
},
{
    "Sid": "IAMAttachRolePermissions",
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy"
    ],
    "Resource": "arn:aws:iam::111122223333:role/DataSync-*",
    "Condition": {
        "ArnLike": {
            "iam:PolicyARN": [
                "arn:aws:iam::111122223333:policy/DataSync-*",
                "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
                "arn:aws:iam::aws:policy/service-role/AWSDataSyncFullAccess"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {

```

```

        "iam:PassedToService": [
            "datasync.amazonaws.com"
        ]
    }
}

```

Tip

Um Ihre Benutzerberechtigungen einzurichten, sollten Sie die Verwendung von [AWSDataSyncFullAccess](#). Dies ist eine AWS verwaltete Richtlinie, die einem Benutzer vollen DataSync und minimalen Zugriff auf seine Abhängigkeiten gewährt.

DataSync service permissions

Der DataSync Dienst benötigt die folgenden Berechtigungen in Ihrem Quellkonto, um Daten in Ihren Zielkonto-Bucket zu übertragen.

Später in diesem Tutorial fügen Sie diese Berechtigungen hinzu, wenn Sie [eine IAM-Rolle für DataSync erstellen](#). Sie geben diese Rolle (*source-datasync-role*) auch in Ihrer [Ziel-Bucket-Richtlinie](#) und bei der [Erstellung Ihres DataSync Zielorts an](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",

```

```
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
]
```

Voraussetzung: Erforderliche Berechtigungen für das Zielkonto

In Ihrem Zielkonto müssen Ihre Benutzerberechtigungen es Ihnen ermöglichen, die Richtlinie Ihres Ziel-Buckets zu aktualisieren und die zugehörigen Zugriffskontrolllisten zu deaktivieren (ACLs). Weitere Informationen zu diesen spezifischen Berechtigungen finden Sie im [Amazon S3 S3-Benutzerhandbuch](#).

Schritt 1: Erstellen Sie in Ihrem Quellkonto einen DataSync Agenten

Zu Beginn müssen Sie einen DataSync Agenten erstellen, der Daten aus Ihrem lokalen Speichersystem lesen und mit dem DataSync Service kommunizieren kann. Dieser Prozess umfasst die Bereitstellung eines Agenten in Ihrer lokalen Speicherumgebung und die Aktivierung des Agenten in Ihrer Quelle. AWS-Konto

Note

Die Schritte in diesem Tutorial gelten für alle Arten von Agenten und Dienstendpunkten, die Sie verwenden.

Um einen DataSync Agenten zu erstellen

1. [Stellen Sie einen DataSync Agenten](#) in Ihrer lokalen Speicherumgebung bereit.
2. [Wählen Sie einen Dienstendpunkt](#) aus, mit AWS dem der Agent kommunizieren soll.
3. [Aktivieren Sie Ihren Agenten](#) in Ihrem Quellkonto.

Schritt 2: Erstellen Sie in Ihrem Quellkonto eine DataSync IAM-Rolle für den Zugriff auf den Ziel-Bucket

In Ihrem Quellkonto benötigen Sie eine IAM-Rolle, die die Berechtigungen zum Übertragen von Daten in DataSync den Bucket Ihres Zielkontos erteilt.

Da Sie Daten kontenübergreifend übertragen, müssen Sie die Rolle manuell erstellen. (DataSync kann diese Rolle für Sie in der Konsole erstellen, wenn Sie sie in demselben Konto übertragen.)

Erstellen Sie die DataSync IAM-Rolle

Erstellen Sie eine IAM-Rolle DataSync als vertrauenswürdige Entität.

So erstellen Sie die IAM-Rolle

1. Melden Sie sich AWS-Managementkonsole mit Ihrem Quellkonto bei der an.
2. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
3. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen und dann Rolle erstellen aus.
4. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option AWS-Service.
5. Wählen Sie DataSync in der Dropdownliste für Anwendungsfall die Option aus und wählen Sie aus DataSync. Wählen Sie Weiter aus.
6. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
7. Geben Sie Ihrer Rolle einen Namen und wählen Sie Rolle erstellen.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Eine Rolle für eine AWS-Service \(Konsole\) erstellen](#).

Fügen Sie der DataSync IAM-Rolle Berechtigungen hinzu

Die IAM-Rolle, die Sie gerade erstellt haben, benötigt die Berechtigungen, die es DataSync ermöglichen, Daten in den S3-Bucket in Ihrem Zielkonto zu übertragen.

So fügen Sie Berechtigungen zu Ihrer IAM-Rolle hinzu

1. Suchen Sie auf der Seite Rollen der IAM-Konsole nach der Rolle, die Sie gerade erstellt haben, und wählen Sie ihren Namen aus.
2. Wählen Sie auf der Detailseite der Rolle den Tab Berechtigungen aus. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
3. Wählen Sie die Registerkarte JSON und gehen Sie wie folgt vor:
 - a. Fügen Sie den folgenden JSON-Code in den Richtlinien-Editor ein:

Note

Der Wert für `aws:ResourceAccount` sollte die Konto-ID sein, der der in der Richtlinie angegebene Amazon S3 S3-Bucket gehört.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",

```

```

        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectTagging"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "123456789012"
        }
    }
}
]
}

```

- b. Ersetzen Sie jede Instanz von *amzn-s3-demo-destination-bucket* durch den Namen des S3-Buckets in Ihrem Zielkonto.
4. Wählen Sie Weiter aus. Geben Sie Ihrer Richtlinie einen Namen und wählen Sie Richtlinie erstellen aus.

Schritt 3: Aktualisieren Sie in Ihrem Zielkonto Ihre S3-Bucket-Richtlinie

Ändern Sie in Ihrem Zielkonto die Ziel-S3-Bucket-Richtlinie so, dass sie die [DataSync IAM-Rolle](#) enthält, die Sie in Ihrem Quellkonto erstellt haben.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die [erforderlichen Berechtigungen für Ihr Zielkonto](#) verfügen.

Um die Ziel-S3-Bucket-Richtlinie zu aktualisieren

1. Wechseln Sie im AWS-Managementkonsole zu Ihrem Zielkonto.
2. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
3. Wählen Sie im linken Navigationsbereich Buckets aus.
4. Wählen Sie in der Bucket-Liste den S3-Bucket aus, in den Sie Daten übertragen möchten.
5. Wählen Sie auf der Detailseite des Buckets den Tab Berechtigungen aus.

6. Wählen Sie unter Bucket-Richtlinie die Option Bearbeiten aus und gehen Sie wie folgt vor, um Ihre S3-Bucket-Richtlinie zu ändern:
 - a. Aktualisieren Sie den Inhalt des Editors, sodass er die folgenden Richtlinienerklärungen enthält:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/source-datasync-role"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

- b. Ersetzen Sie jede Instanz von *source-account* durch die AWS-Konto ID Ihres Quellkontos.
- c. *source-datasync-role* Ersetzen Sie sie durch die [IAM-Rolle, für die Sie DataSync in Ihrem Quellkonto erstellt](#) haben.

- d. Ersetzen Sie jede Instanz von *amzn-s3-demo-destination-bucket* durch den Namen des S3-Buckets in Ihrem Zielkonto.
7. Wählen Sie **Änderungen speichern** aus.

Schritt 4: Deaktivieren Sie in Ihrem Zielkonto die Option ACLs für Ihren S3-Bucket

Es ist wichtig, dass alle Daten, die Sie in den S3-Bucket kopieren, zu Ihrem Zielkonto gehören. Um sicherzustellen, dass dieses Konto Eigentümer der Daten ist, deaktivieren Sie die Zugriffskontrolllisten des Buckets (ACLs). Weitere Informationen finden Sie unter [Kontrolle des Besitzes von Objekten und Deaktivierung ACLs für Ihren Bucket](#) im Amazon S3 S3-Benutzerhandbuch.

Zur Deaktivierung ACLs für Ihren Ziel-Bucket

1. Während Sie immer noch mit Ihrem Zielkonto an der S3-Konsole angemeldet sind, wählen Sie den S3-Bucket aus, in den Sie Daten übertragen möchten.
2. Wählen Sie auf der Detailseite des Buckets den Tab **Berechtigungen** aus.
3. Wählen Sie unter **Object Ownership** die Option **Edit (Bearbeiten)**.
4. Falls sie noch nicht ausgewählt ist, wählen Sie die **ACLs deaktiviert** (empfohlene) Option.
5. Wählen Sie **Änderungen speichern** aus.

Schritt 5: Erstellen Sie in Ihrem Quellkonto einen DataSync Quellspeicherort für Ihren lokalen Speicher

Erstellen Sie in Ihrem Quellkonto einen [DataSync Quellspeicherort](#) für das lokale Speichersystem, von dem Sie Daten übertragen. Dieser Standort verwendet den [Agenten, den Sie in Ihrem Quellkonto aktiviert](#) haben.

Schritt 6: Erstellen Sie in Ihrem Quellkonto einen DataSync Zielort für Ihren S3-Bucket

Erstellen Sie, solange Sie sich noch in Ihrem Quellkonto befinden, einen Speicherort für den S3-Bucket, in den Sie Daten übertragen.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die [erforderlichen Berechtigungen für Ihr Quellkonto](#) verfügen.

Da Sie mit der DataSync Konsolenoberfläche keine kontoübergreifenden Standorte erstellen können, müssen Sie für diese Anweisungen einen `create-location-s3` Befehl ausführen, um Ihren Zielstandort zu erstellen. Wir empfehlen, den Befehl mithilfe einer browserbasierten AWS CloudShell, vorab authentifizierten Shell auszuführen, die Sie direkt von der Konsole aus starten. CloudShell ermöglicht es Ihnen, AWS CLI Befehle auszuführen, `create-location-s3` ohne Befehlszeilentools herunterzuladen oder zu installieren.

 Note

Um die folgenden Schritte mit einem anderen Befehlszeilentool als auszuführen CloudShell, stellen Sie sicher, dass Ihr [AWS CLI Profil](#) dieselbe IAM-Rolle verwendet, die die [erforderlichen Benutzerberechtigungen für](#) die Verwendung DataSync in Ihrem Quellkonto enthält.

Um einen DataSync Zielort zu erstellen, verwenden Sie CloudShell

1. Wenn Sie sich noch in Ihrem Quellkonto befinden, führen Sie einen der folgenden Schritte aus, um CloudShell von der Konsole aus zu starten:
 - Wählen Sie das CloudShell Symbol in der Navigationsleiste der Konsole. Es befindet sich rechts neben dem Suchfeld.
 - Verwenden Sie das Suchfeld in der Navigationsleiste der Konsole, um nach der CloudShellOption zu suchen CloudShellund diese dann auszuwählen.
2. Kopieren Sie den folgenden Befehl:

```
aws datasync create-location-s3 \  
  --s3-bucket-arn arn:aws:s3:::amzn-s3-demo-destination-bucket \  
  --s3-config '{  
    "BucketAccessRoleArn":"arn:aws:iam::source-user-account:role/source-datasync-  
role"  
  }'
```

3. *amzn-s3-demo-destination-bucket* Ersetzen Sie ihn durch den Namen des S3-Buckets in Ihrem Zielkonto.
4. *source-user-account* Ersetzen Sie es durch die AWS-Konto ID für Ihr Quellkonto.

5. `source-datasync-role` Ersetzen Sie durch die [DataSync IAM-Rolle](#), die Sie in Ihrem Quellkonto erstellt haben.
6. Führen Sie den Befehl in CloudShell aus.

Wenn der Befehl einen ähnlichen DataSync Standort-ARN zurückgibt, haben Sie den Standort erfolgreich erstellt:

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
abcdef01234567890"
}
```

7. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.

In Ihrem Quellkonto können Sie den S3-Standort sehen, den Sie gerade für Ihren Zielkonto-Bucket erstellt haben.

Schritt 7: Erstellen und starten Sie in Ihrem Quellkonto Ihre DataSync Aufgabe

Bevor Sie eine DataSync Aufgabe zur Übertragung Ihrer Daten starten, lassen Sie uns zusammenfassen, was Sie bisher getan haben:

- In Ihrem Quellkonto haben Sie Ihren DataSync Agenten erstellt. Der Agent kann aus Ihrem lokalen Speichersystem lesen und mit dem DataSync Service kommunizieren.
- In Ihrem Quellkonto haben Sie eine IAM-Rolle erstellt, die es ermöglicht DataSync , Daten in den S3-Bucket in Ihrem Zielkonto zu übertragen.
- In Ihrem Zielkonto haben Sie Ihren S3-Bucket so konfiguriert, dass Daten dorthin übertragen werden DataSync können.
- In Ihrem Quellkonto haben Sie die DataSync Quell- und Zielorte für Ihre Übertragung erstellt.

Um die DataSync Aufgabe zu erstellen und zu starten

1. Wenn Sie weiterhin die DataSync Konsole in Ihrem Quellkonto verwenden, erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Aufgaben und Aufgabe erstellen aus.

2. Wählen Sie auf der Seite Quellspeicherort konfigurieren die Option Vorhandenen Speicherort auswählen aus. Wählen Sie den Quellspeicherort aus, von dem Sie Daten kopieren möchten (Ihr lokaler Speicher), und klicken Sie dann auf Weiter.
3. Wählen Sie auf der Seite Zielort konfigurieren die Option Vorhandenen Speicherort auswählen aus. Wählen Sie den Zielort aus, an den Sie Daten kopieren möchten (den S3-Bucket in Ihrem Zielkonto), und klicken Sie dann auf Weiter.
4. Geben Sie der Aufgabe auf der Seite „Einstellungen konfigurieren“ einen Namen. Konfigurieren Sie bei Bedarf zusätzliche Einstellungen, z. B. die Angabe einer CloudWatch Amazon-Protokollgruppe. Wählen Sie Weiter aus.
5. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Einstellungen und wählen Sie „Aufgabe erstellen“.
6. Wählen Sie auf der Detailseite der Aufgabe die Option Start und dann eine der folgenden Optionen aus:
 - Um die Aufgabe ohne Änderungen auszuführen, wählen Sie Mit Standardeinstellungen beginnen.
 - Um die Aufgabe vor der Ausführung zu ändern, wählen Sie Mit überschreibenden Optionen beginnen.

Wenn Ihre Aufgabe abgeschlossen ist, überprüfen Sie den S3-Bucket in Ihrem Zielkonto. Sie sollten die Daten sehen, die von Ihrem Quellstandort verschoben wurden.

Zugehörige Ressourcen

Weitere Informationen dazu, was Sie in diesem Tutorial gemacht haben, finden Sie in den folgenden Themen:

- [Eine Rolle für eine AWS-Service \(Konsole\) erstellen](#)
- [Änderung einer Vertrauensrichtlinie für Rollen \(Konsole\)](#)
- [Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole](#)
- [Erstellen Sie einen S3-Standort mit dem AWS CLI](#)

Tutorial: Daten zwischen Amazon S3 S3-Buckets übertragen AWS-Konten

Mit AWS DataSync können Sie Daten zwischen Amazon S3 S3-Buckets übertragen, die zu unterschiedlichen AWS-Konten gehören.

Important

Die Übertragung von Daten AWS-Konten mit den Methoden in diesem Tutorial funktioniert nur mit Amazon S3. Darüber hinaus kann Ihnen dieses Tutorial dabei helfen, Daten zwischen S3-Buckets zu übertragen, die sich ebenfalls in unterschiedlichen AWS-Regionen Bereichen befinden.

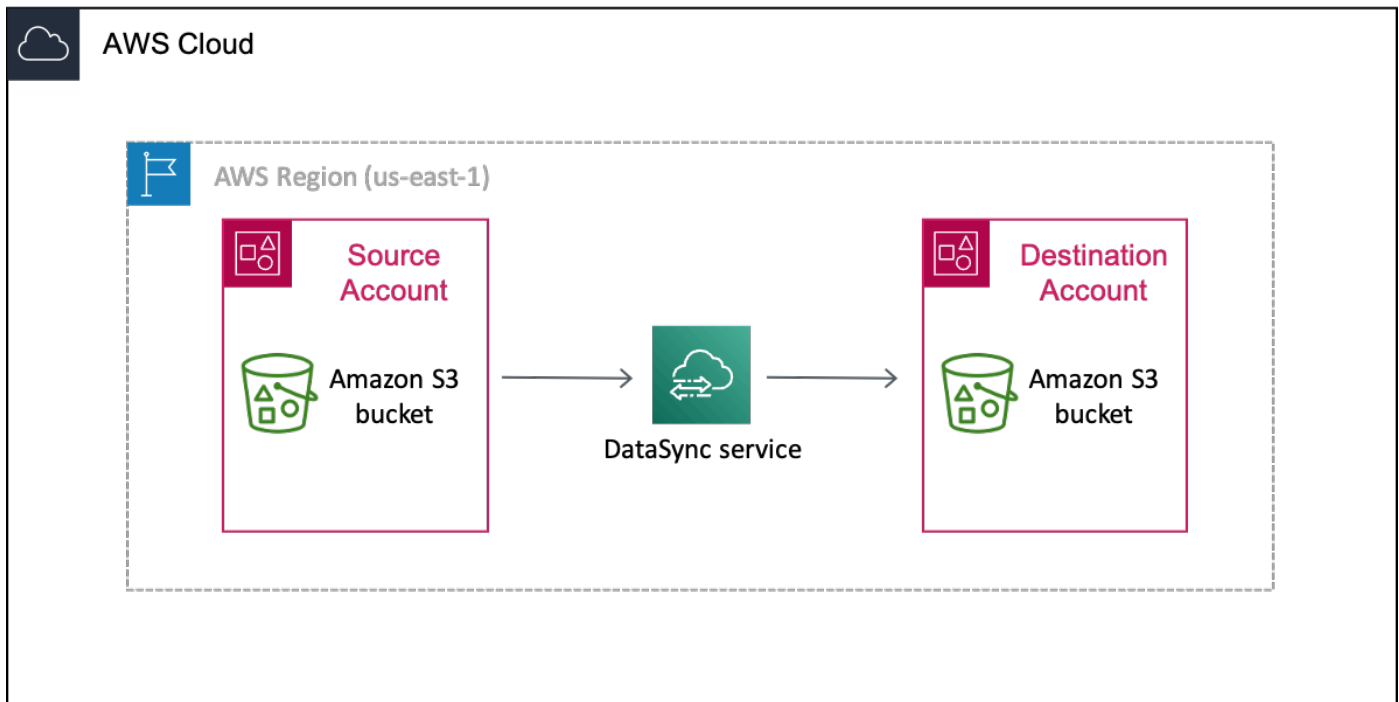
-Übersicht

Es ist nicht ungewöhnlich, Daten zwischen ihnen zu übertragen AWS-Konten, insbesondere wenn Sie separate Teams haben, die die Ressourcen Ihres Unternehmens verwalten. So kann eine kontoübergreifende Übertragung DataSync mithilfe von:

- Quellkonto: Das Konto AWS-Konto für die Verwaltung des S3-Buckets, aus dem Sie Daten übertragen müssen.
- Zielkonto: Das Konto AWS-Konto für die Verwaltung des S3-Buckets, in den Sie Daten übertragen müssen.

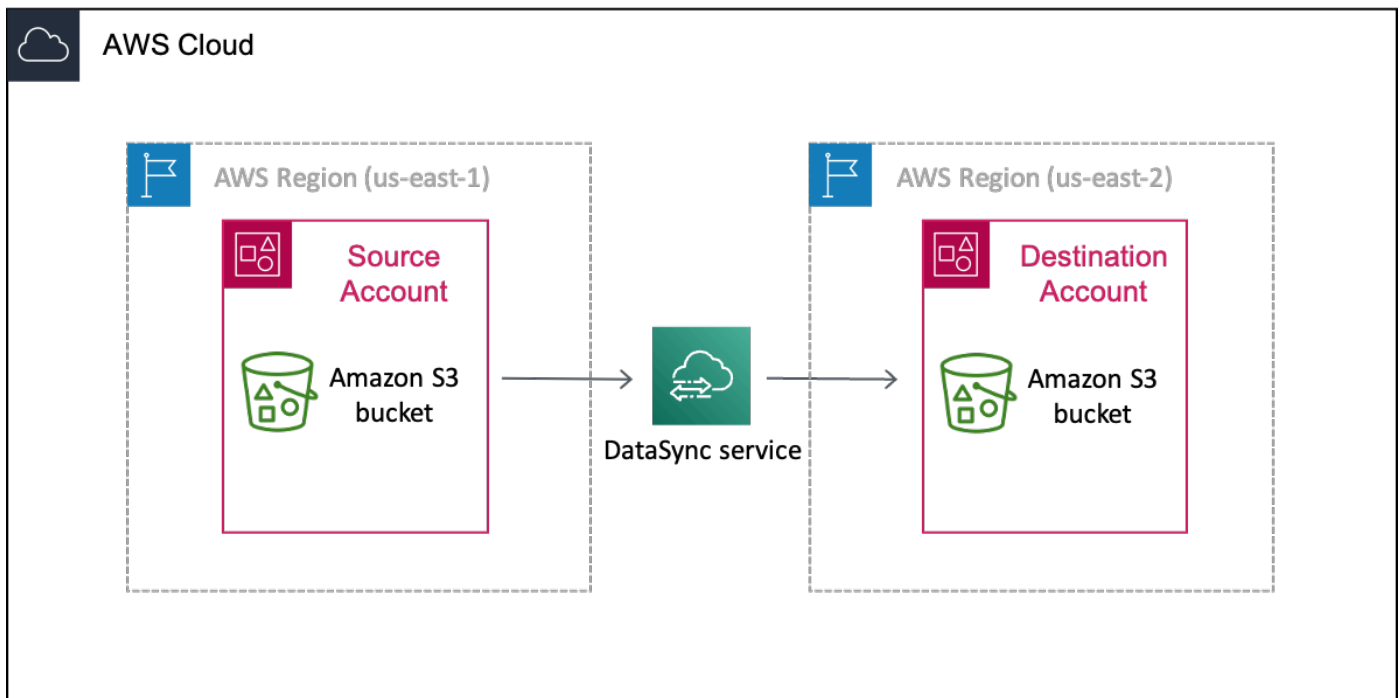
Transfers across accounts

Das folgende Diagramm zeigt ein Szenario, in dem Sie Daten von einem S3-Bucket in einen anderen S3-Bucket übertragen, der sich in einem anderen befindet AWS-Konto.



Transfers across accounts and Regions

Das folgende Diagramm zeigt ein Szenario, in dem Sie Daten von einem S3-Bucket in einen anderen S3-Bucket übertragen, der sich in einer anderen AWS-Konto AND-Region befindet.



Voraussetzung: Erforderliche Quellkontoberechtigungen

Für Ihre Quelle AWS-Konto sind bei dieser Art der kontoübergreifenden Übertragung zwei Arten von Berechtigungen zu berücksichtigen:

- Benutzerberechtigungen, mit denen ein Benutzer arbeiten kann DataSync (dies können Sie oder Ihr Speicheradministrator sein). Mit diesen Berechtigungen können Sie DataSync Standorte und Aufgaben erstellen.
- DataSync Serviceberechtigungen, die es DataSync ermöglichen, Daten in den Bucket Ihres Zielkontos zu übertragen.

Benutzerberechtigungen für Ihr Quellkonto

Fügen Sie in Ihrem Quellkonto mindestens die folgenden Berechtigungen zu einer IAM-Rolle hinzu, um Ihre DataSync Standorte und Aufgaben zu erstellen. Informationen zum Hinzufügen von Berechtigungen zu einer Rolle finden Sie unter Eine IAM-Rolle [erstellen](#) oder [ändern](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SourceUserRolePermissions",
      "Effect": "Allow",
      "Action": [
        "datasync:CreateLocationS3",
        "datasync:CreateTask",
        "datasync:DescribeLocation*",
        "datasync:DescribeTaskExecution",
        "datasync:ListLocations",
        "datasync:ListTaskExecutions",
        "datasync:DescribeTask",
        "datasync:CancelTaskExecution",
        "datasync:ListTasks",
        "datasync:StartTaskExecution",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    }
  ]
}
```



```

    },
    {
      "Sid": "IAMPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:ListRoles",
        "iam:CreatePolicy"
      ],
      "Resource": "arn:aws:iam::111122223333:role/DataSync-*"
    },
    {
      "Sid": "IAMAttachRolePermissions",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy"
      ],
      "Resource": "arn:aws:iam::111122223333:role/DataSync-*",
      "Condition": {
        "ArnLike": {
          "iam:PolicyARN": [
            "arn:aws:iam::111122223333:policy/DataSync-*",
            "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
            "arn:aws:iam::aws:policy/service-role/AWSDataSyncFullAccess"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": [
            "datasync.amazonaws.com"
          ]
        }
      }
    }
  ]

```

```
}
```

Tip

Um Ihre Benutzerberechtigungen einzurichten, sollten Sie die Verwendung von [AWSDataSyncFullAccess](#). Dies ist eine AWS verwaltete Richtlinie, die einem Benutzer vollen DataSync und minimalen Zugriff auf seine Abhängigkeiten gewährt.

DataSync Serviceberechtigungen für Ihr Quellkonto

Der DataSync Dienst benötigt die folgenden Berechtigungen in Ihrem Quellkonto, um Daten in den Bucket Ihres Zielkontos zu übertragen.

Später in diesem Tutorial fügen Sie diese Berechtigungen hinzu, wenn Sie [eine IAM-Rolle für DataSync erstellen](#). Sie geben diese Rolle (*source-datasync-role*) auch in Ihrer [Ziel-Bucket-Richtlinie](#) und bei der [Erstellung Ihres DataSync Zielorts an](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",

```

```
    "s3:PutObjectTagging"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
]
```

Voraussetzung: Erforderliche Berechtigungen für das Zielkonto

In Ihrem Zielkonto müssen Ihre Benutzerberechtigungen es Ihnen ermöglichen, die Richtlinie Ihres Ziel-Buckets zu aktualisieren und die zugehörigen Zugriffskontrolllisten zu deaktivieren (ACLs). Weitere Informationen zu diesen spezifischen Berechtigungen finden Sie im [Amazon S3 S3-Benutzerhandbuch](#).

Schritt 1: Erstellen Sie in Ihrem Quellkonto eine DataSync IAM-Rolle für den Zugriff auf den Ziel-Bucket

In Ihrer Quelle benötigen Sie eine IAM-Rolle AWS-Konto, die die Berechtigungen zum Übertragen von Daten in DataSync den Bucket Ihres Zielkontos erteilt.

Da Sie Daten zwischen Konten übertragen, müssen Sie die Rolle manuell erstellen. (DataSync kann diese Rolle für Sie in der Konsole erstellen, wenn Sie sie in demselben Konto übertragen.)

Erstellen Sie die DataSync IAM-Rolle

Erstellen Sie eine IAM-Rolle DataSync als vertrauenswürdige Entität.

1. Melden Sie sich AWS-Managementkonsole mit Ihrem Quellkonto bei der an.
2. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
3. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen und dann Rolle erstellen aus.
4. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option AWS-Service.
5. Wählen Sie DataSync in der Dropdownliste für Anwendungsfall die Option aus und wählen Sie aus DataSync. Wählen Sie Weiter aus.
6. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.

7. Geben Sie Ihrer Rolle einen Namen und wählen Sie Rolle erstellen.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Eine Rolle für eine AWS-Service \(Konsole\) erstellen](#).

Fügen Sie der DataSync IAM-Rolle Berechtigungen hinzu

Die IAM-Rolle, die Sie gerade erstellt haben, benötigt die Berechtigungen, die es DataSync ermöglichen, Daten in den S3-Bucket in Ihrem Zielkonto zu übertragen.

1. Suchen Sie auf der Seite Rollen der IAM-Konsole nach der Rolle, die Sie gerade erstellt haben, und wählen Sie ihren Namen aus.
2. Wählen Sie auf der Detailseite der Rolle den Tab Berechtigungen aus. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
3. Wählen Sie die Registerkarte JSON und gehen Sie wie folgt vor:
 - a. Fügen Sie den folgenden JSON-Code in den Richtlinien-Editor ein:

Note

Der Wert für `aws:ResourceAccount` sollte die Konto-ID sein, der der in der Richtlinie angegebene Amazon S3 S3-Bucket gehört.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
      "Condition": {
        "StringEquals": {
```

```

        "aws:ResourceAccount": "123456789012"
      }
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}

```

- b. Ersetzen Sie jede Instanz von *amzn-s3-demo-destination-bucket* durch den Namen des S3-Buckets in Ihrem Zielkonto.
4. Wählen Sie Weiter aus. Geben Sie Ihrer Richtlinie einen Namen und wählen Sie Richtlinie erstellen aus.

Schritt 2: Aktualisieren Sie in Ihrem Zielkonto Ihre S3-Bucket-Richtlinie

Ändern Sie in Ihrem Zielkonto die Ziel-S3-Bucket-Richtlinie so, dass sie die [DataSync IAM-Rolle](#) enthält, die Sie in Ihrem Quellkonto erstellt haben.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die [erforderlichen Berechtigungen für Ihr Zielkonto](#) verfügen.

Aktualisieren Sie Ihre S3-Bucket-Richtlinie für Ihr Ziel

1. Wechseln Sie im AWS-Managementkonsole zu Ihrem Zielkonto.
2. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
3. Wählen Sie im linken Navigationsbereich Buckets aus.
4. Wählen Sie in der Bucket-Liste den S3-Bucket aus, in den Sie Daten übertragen möchten.
5. Wählen Sie auf der Detailseite des Buckets den Tab Berechtigungen aus.
6. Wählen Sie unter Bucket-Richtlinie die Option Bearbeiten aus und gehen Sie wie folgt vor, um Ihre S3-Bucket-Richtlinie zu ändern:
 - a. Aktualisieren Sie den Inhalt des Editors, sodass er die folgenden Richtlinienerklärungen enthält:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/source-datasync-role"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

```
}  
  ]  
}
```

- b. Ersetzen Sie jede Instanz von *source-account* durch die AWS-Konto ID Ihres Quellkontos.
 - c. *source-datasync-role* Ersetzen Sie sie durch die [IAM-Rolle, für die Sie DataSync in Ihrem Quellkonto erstellt](#) haben.
 - d. Ersetzen Sie jede Instanz von *amzn-s3-demo-destination-bucket* durch den Namen des S3-Buckets in Ihrem Zielkonto.
7. Wählen Sie **Änderungen speichern** aus.

Schritt 3: Deaktivieren Sie in Ihrem Zielkonto die Option ACLs für Ihren S3-Bucket

Es ist wichtig, dass alle Daten, die Sie in den S3-Bucket übertragen, zu Ihrem Zielkonto gehören. Um sicherzustellen, dass dieses Konto Eigentümer der Daten ist, deaktivieren Sie die Zugriffskontrolllisten des Buckets (ACLs). Weitere Informationen finden Sie unter [Kontrolle des Besitzes von Objekten und Deaktivierung ACLs für Ihren Bucket](#) im Amazon S3 S3-Benutzerhandbuch.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die [erforderlichen Berechtigungen für Ihr Zielkonto](#) verfügen.

Deaktivieren Sie Ihren Ziel-S3-Bucket ACLs

1. Während Sie immer noch mit Ihrem Zielkonto an der S3-Konsole angemeldet sind, wählen Sie den S3-Bucket aus, in den Sie Daten übertragen möchten.
2. Wählen Sie auf der Detailseite des Buckets den Tab **Berechtigungen** aus.
3. Wählen Sie unter Object Ownership die Option **Edit** (Bearbeiten).
4. Falls sie noch nicht ausgewählt ist, wählen Sie die **ACLs deaktiviert** (empfohlene) Option.
5. Wählen Sie **Änderungen speichern** aus.

Schritt 4: Erstellen Sie in Ihrem Quellkonto Ihre DataSync Standorte

Erstellen Sie in Ihrem Quellkonto die DataSync Standorte für Ihre S3-Quell- und Ziel-Buckets.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die [erforderlichen Berechtigungen für Ihr Quellkonto](#) verfügen.

Erstellen Sie Ihren DataSync Quellstandort

- Erstellen Sie in Ihrem Quellkonto einen [Speicherort](#) für den S3-Bucket, aus dem Sie Daten übertragen.

Erstellen Sie Ihren DataSync Zielort

Erstellen Sie, solange Sie sich noch in Ihrem Quellkonto befinden, einen Speicherort für den S3-Bucket, in den Sie Daten übertragen.

Da Sie mit der DataSync Konsolenoberfläche keine kontoübergreifenden Standorte erstellen können, müssen Sie für diese Anweisungen einen `create-location-s3` Befehl ausführen, um Ihren Zielstandort zu erstellen. Wir empfehlen, den Befehl mithilfe einer browserbasierten AWS CloudShell, vorab authentifizierten Shell auszuführen, die Sie direkt von der Konsole aus starten. CloudShellermöglicht es Ihnen, AWS CLI Befehle auszuführen, `create-location-s3` ohne Befehlszeilentools herunterzuladen oder zu installieren.

 Note

Um die folgenden Schritte mit einem anderen Befehlszeilentool als auszuführen CloudShell, stellen Sie sicher, dass Ihr [AWS CLI Profil](#) dieselbe IAM-Rolle verwendet, die die [erforderlichen Benutzerberechtigungen für](#) die Verwendung DataSync in Ihrem Quellkonto enthält.

Um einen DataSync Zielort zu erstellen, verwenden Sie CloudShell

1. Wenn Sie sich noch in Ihrem Quellkonto befinden, führen Sie einen der folgenden Schritte aus, um CloudShell von der Konsole aus zu starten:
 - Wählen Sie das CloudShell Symbol in der Navigationsleiste der Konsole. Es befindet sich rechts neben dem Suchfeld.
 - Verwenden Sie das Suchfeld in der Navigationsleiste der Konsole, um nach der CloudShellOption zu suchen CloudShellund diese dann auszuwählen.
2. Kopieren Sie den folgenden `create-location-s3` Befehl:


```
aws datasync create-location-s3 \
  --s3-bucket-arn arn:aws:s3:::amzn-s3-demo-destination-bucket \
  --region amzn-s3-demo-destination-bucket-region \
  --s3-config '{
    "BucketAccessRoleArn": "arn:aws:iam::source-account-id:role/source-datasync-
role"
  }'
```

3. *amzn-s3-demo-destination-bucket* Ersetzen Sie ihn durch den Namen des S3-Buckets in Ihrem Zielkonto.
4. Wenn sich Ihr Ziel-Bucket in einer anderen Region als Ihr Quell-Bucket befindet, *amzn-s3-demo-destination-bucket-region* ersetzen Sie es durch die Region, in der sich der Ziel-Bucket befindet (z. B. *us-east-2*). Entfernen Sie diese Option, wenn sich Ihre Buckets in derselben Region befinden.
5. Ersetzen Sie es *source-account-id* durch die AWS-Konto Quell-ID.
6. *source-datasync-role* Ersetzen Sie durch die [DataSyncIAM-Rolle](#), die Sie in Ihrem Quellkonto erstellt haben.
7. Führen Sie den Befehl in CloudShell aus.

Wenn der Befehl einen ähnlichen DataSync Standort-ARN zurückgibt, haben Sie den Standort erfolgreich erstellt:

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
abcdef01234567890"
}
```

8. Erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Standorte aus.
9. Wenn Sie den Standort in einer anderen Region erstellt haben, wählen Sie diese Region im Navigationsbereich aus.

In Ihrem Quellkonto können Sie den S3-Standort sehen, den Sie gerade für Ihren Zielkonto-Bucket erstellt haben.

Schritt 5: Erstellen und starten Sie in Ihrem Quellkonto Ihre DataSync Aufgabe

Bevor Sie eine DataSync Aufgabe zur Übertragung Ihrer Daten starten, lassen Sie uns zusammenfassen, was Sie bisher getan haben:

- In Ihrem Quellkonto haben Sie eine IAM-Rolle erstellt, die es ermöglicht DataSync , Daten in den S3-Bucket in Ihrem Zielkonto zu übertragen.
- In Ihrem Zielkonto haben Sie Ihren S3-Bucket so konfiguriert, dass Daten dorthin übertragen werden DataSync können.
- In Ihrem Quellkonto haben Sie die DataSync Quell- und Zielorte für Ihre Übertragung erstellt.

Erstelle und starte deine DataSync Aufgabe

1. Während Sie weiterhin die DataSync Konsole in Ihrem Quellkonto verwenden, erweitern Sie im linken Navigationsbereich die Option Datenübertragung und wählen Sie dann Aufgaben und Aufgabe erstellen aus.
2. Wenn sich der Bucket in Ihrem Zielkonto in einer anderen Region befindet als der Bucket in Ihrem Quellkonto, wählen Sie im oberen Navigationsbereich die Region des Ziel-Buckets aus.

Important

Um einen Netzwerkverbindungsfehler zu vermeiden, müssen Sie Ihre DataSync Aufgabe in derselben Region wie der Zielort erstellen.

3. Gehen Sie auf der Seite Quellspeicherort konfigurieren wie folgt vor:
 - a. Wählen Sie Bestehenden Standort auswählen aus.
 - b. (Für regionsübergreifende Übertragungen) Wählen Sie in der Dropdownliste Region die Region aus, in der sich der Quell-Bucket befindet.
 - c. Wählen Sie für Bestehende Standorte den Quellstandort für den S3-Bucket aus, aus dem Sie Daten übertragen, und wählen Sie dann Weiter aus.
4. Gehen Sie auf der Seite Zielort konfigurieren wie folgt vor:
 - a. Wählen Sie Bestehenden Standort auswählen aus.

- b. Wählen Sie unter Bestehende Standorte den Zielort für den S3-Bucket aus, an den Sie Daten übertragen, und wählen Sie dann Weiter aus.
5. Wählen Sie auf der Seite „Einstellungen konfigurieren“ einen Aufgabenmodus aus.

 Tip

Wir empfehlen, den erweiterten Modus zu verwenden. Weitere Informationen finden Sie unter [Wählen Sie einen Aufgabenmodus für Ihre Datenübertragung](#).

6. Geben Sie der Aufgabe einen Namen und konfigurieren Sie zusätzliche Einstellungen, z. B. die Angabe einer CloudWatch Amazon-Protokollgruppe. Wählen Sie Weiter aus.
7. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Einstellungen und wählen Sie „Aufgabe erstellen“.
8. Wählen Sie auf der Detailseite der Aufgabe die Option Start und dann eine der folgenden Optionen aus:
 - Um die Aufgabe ohne Änderungen auszuführen, wählen Sie Mit Standardeinstellungen beginnen.
 - Um die Aufgabe vor der Ausführung zu ändern, wählen Sie Mit überschreibenden Optionen beginnen.

Wenn Ihre Aufgabe abgeschlossen ist, überprüfen Sie den S3-Bucket in Ihrem Zielkonto. Sie sollten die Daten sehen, die aus Ihrem Quellkonto-Bucket verschoben wurden.

Fehlerbehebung

Lesen Sie die folgenden Informationen, falls Sie beim Versuch, Ihre kontoübergreifende Übertragung abzuschließen, auf Probleme stoßen.

Verbindungsfehler

Bei der Übertragung zwischen S3-Buckets in verschiedenen Regionen AWS-Konten und in Regionen mit Aufgaben im Basismodus wird möglicherweise ein Netzwerkverbindungsfehler angezeigt, wenn Sie Ihre DataSync Aufgabe starten. Um dieses Problem zu beheben, verwenden Sie eine Aufgabe im erweiterten Modus. Alternativ können Sie eine Aufgabe im Basismodus in derselben Region wie Ihr Zielstandort erstellen und versuchen, diese Aufgabe auszuführen.

Verwandt: Kontoübergreifende Übertragungen mit S3-Buckets unter Verwendung serverseitiger Verschlüsselung

[Wenn Sie versuchen, diese Übertragung mit S3-Buckets unter Verwendung serverseitiger Verschlüsselung durchzuführen, finden Sie Anweisungen im AWS Storage-Blog.](#)

Durchführung einer großen Datenmigration mit AWS DataSync

Umfangreiche Datenmigrationen können die Übertragung großer Datenmengen beinhalten, die Millionen von Dateien oder Objekten in verschiedenen Formaten umfassen. AWS DataSync vereinfacht diese komplexen Übertragungen durch Verwaltung der Planung, Überwachung, Verschlüsselung und Datenüberprüfung.

Was ist eine umfangreiche Datenmigration?

Eine umfangreiche Datenmigration beinhaltet in der Regel die Übertragung von Terabyte oder mehr an Daten, die über verschiedene Quellen verteilt sind, in eine neue Zielspeicherumgebung (in diesem Fall AWS). Diese Migrationen erfordern eine sorgfältige Planung und Koordination innerhalb Ihres Unternehmens, um Daten erfolgreich zu verschieben und gleichzeitig Betriebsunterbrechungen zu minimieren.

DataSync kann diese Migrationen vereinfachen, die in der Regel komplexer Natur sind. Zu den Vorteilen der Verwendung DataSync für Ihre Migration gehören:

- Automatisierte Verwaltung der Datenübertragungsprozesse und der Infrastruktur, die für leistungsstarke und sichere Datenübertragungen erforderlich sind.
- End-to-end Sicherheit, einschließlich Verschlüsselung und Überprüfung der Datenintegrität, um sicherzustellen, dass Ihre Daten sicher, unversehrt und einsatzbereit ankommen.
- Ein speziell entwickeltes Netzwerkprotokoll und eine parallel Multithread-Architektur zur Beschleunigung von Migrationen.

Die wichtigsten Phasen einer Migration großer Datenmengen

In der Regel können Sie eine umfangreiche Migration in die folgenden Phasen unterteilen:

- (Phase 1) Planung Ihrer Datenmigration — In dieser Phase versuchen Sie zu verstehen, warum Sie migrieren und mit welcher Art von Daten Sie arbeiten. Zu den Planungsaktivitäten gehören:
 - Verstehen, warum Sie migrieren möchten
 - Zusammenstellung eines Teams, das Sie bei allen Aspekten der Migration unterstützt.
 - Identifizierung von Datenstandorten, Formaten und Nutzungsmustern

- Bewertung der verfügbaren Hardwareressourcen und Netzwerkanforderungen (wenn Sie von einem lokalen Rechenzentrum aus migrieren)
- Durchführung von Machbarkeitsstudien (POC) mit dem Ziel, die Zeitpläne für die Migration DataSync abzuschätzen, Zeitfenster für die Umstellung zu planen und ein Gefühl dafür zu bekommen, wie Sie die Konfiguration vornehmen müssen DataSync
- (Phase 2) Implementierung Ihrer Migration großer Datenmengen — Zu diesem Zeitpunkt validieren Sie Ihren Plan und beginnen mit der Migration. Zu den Implementierungsaktivitäten gehören:
 - Validierung des Migrationsplans
 - Durchführung schrittweiser Umstellungen, die die erwartungsgemäße Überwachung und Überprüfung Ihrer Datenübertragungen beinhalten
 - Optimierung und Anpassung nach Bedarf zwischen den einzelnen Umstellungen
 - Bereinigen Sie ungenutzte Ressourcen, sobald Sie fertig sind

Weitere Ressourcen

AWS Prescriptive Guidance bietet die folgenden Ressourcen, die Ihnen bei der Planung und Implementierung einer großen Migration helfen können. Anhand dieses Leitfadens erfahren Sie, wie DataSync Sie im Kontext gängiger Migrationsprozesse und -aktivitäten vorgehen können.

- [Große Migrationen in die Cloud AWS](#)
- [Strategie und bewährte Methoden für große Migrationen AWS](#)
- [Migrieren Sie gemeinsam genutzte Dateisysteme in einer AWS großen Migration](#) — Diese Ressource enthält eine SFS-Discovery-Arbeitsmappe, die Sie herunterladen und verwenden können, um eine Migration auf Dateifreigabeebene zu planen.

Phase 1: Planung Ihrer Migration großer Datenmengen

Die Planung ist bei der Migration eines großen Datensatzes unerlässlich. Sie müssen wissen, welche Daten Sie migrieren, welche Beweggründe Sie für die Migration hatten und wie wir Ihnen helfen AWS DataSync können, Ihre Daten dorthin zu bringen, wo Sie sie haben möchten.

Themen

- [Erfassung der Anforderungen für Ihre Migration](#)
- [Durchführung eines DataSync Machbarkeitsnachweises](#)

- [Schätzung der Migrationszeitpläne](#)

Erfassung der Anforderungen für Ihre Migration

Der erste Schritt bei einer großen Datenmigration erfordert die Erfassung einer Vielzahl von Informationen in Ihrem Unternehmen.

Diese Informationen helfen Ihnen bei der Erstellung eines [Migrationsprozesses](#), der bei umfangreichen Migrationen mehrere Übertragungen und Verfahren zur Übertragung von Vorgängen (in [Wellen](#)) von Ihrem Quell- auf Ihren Zielspeicher umfassen kann.

Verstehen Sie, warum Sie migrieren möchten

Bevor Sie mit der Migration zu beginnen AWS, müssen Sie genau verstehen, warum Sie Ihre Daten migrieren. Dies hilft bei der Bewältigung gängiger Migrationsherausforderungen wie der Einhaltung von Fristen, der Verwaltung von Ressourcen und der teamübergreifenden Koordination.

Wenn Sie Hilfe bei der Ermittlung Ihrer Beweggründe für die Migration benötigen, beantworten Sie diese Fragen:

- Geben Sie lokalen Speicherplatz frei?
- Halten Sie die Vertragsfristen für Hardwaresupport ein?
- Ist das für den Ausgang eines Rechenzentrums?
- Was ist Ihr Zeitplan für die Migration?
- Übertragen Sie Daten aus einem anderen Cloud-Speicher?
- Migrieren Sie teilweise oder vollständige Datensätze?
- Ist das für die Datenarchivierung?
- Benötigen Anwendungen oder Benutzer regelmäßigen Zugriff auf diese Daten?

Die Logistik herausfinden

Gehen Sie auf einige grundlegende logistische Fragen zu Ihrer Speicherumgebung, der Migration und Ihrer Organisation ein:

1. Verschaffen Sie sich ein grundlegendes Verständnis Ihrer aktuellen Datenspeicherinfrastruktur.
2. Prüfen Sie, ob Sie einen [DataSync Agenten](#) benötigen. Sie benötigen beispielsweise einen Agenten, wenn Sie Daten aus einem lokalen Speicher übertragen.

3. Wenn Sie einen Agenten benötigen, stellen Sie sicher, dass Sie die [Anforderungen des Agenten](#) verstehen:
 - Ein Agent kann als virtuelle Maschine (VM) VMware ESXi, Linux-Kernel-basierte virtuelle Maschine (KVM) und als Microsoft Hyper-V-Hypervisoren ausgeführt werden. Sie können einen Agenten auch als EC2 Amazon-Instance innerhalb bereitstellen AWS.
 - Große Migrationen sind in der Regel speicherintensiv. Stellen Sie sicher, dass Ihr Agent über ausreichend RAM verfügt.
4. Identifizieren Sie die wichtigsten Stakeholder aus Ihren Führungskräften, Netzwerk-, Speicher- und IT-Abteilungen, die an der Migration beteiligt werden müssen. Dazu können folgende Angaben zählen:
 - Finden Sie [einen Ansprechpartner, der](#) sich ausschließlich mit dem Projekt und seinen Ergebnissen befasst.
 - Ermitteln Sie, wer für den Besitz und die Klassifizierung der Daten verantwortlich ist, die Sie migrieren.
 - Identifizieren Sie, wer Ihre Quelle verwaltet und wer letztendlich den AWS Speicherservice verwaltet, zu dem Sie migrieren.
 - Finden Sie heraus, wer weitere Prozesse für Ihre Daten erstellt und verwaltet, sobald sie eingegangen sind. AWS
5. Richten Sie abteilungsübergreifende Kommunikationskanäle ein.
6. Erstellen Sie einen Rollback-Plan für Eventualitäten.
7. Dokumentieren Sie den gesamten Migrationsprozess, einschließlich der Phasen-, Validierungs- und Umstellungsverfahren. Verwenden Sie dies als Ihr Runbook für die gesamte Migration. Sie werden diesen Prozess bei der Planung und Implementierung der Migration aktualisieren.

Überprüfung der Daten, die Sie migrieren

Analysieren Sie gemeinsam mit Ihren Speicher- und Anwendungsteams die Eigenschaften der Daten, die Sie migrieren möchten. Diese Informationen helfen Ihnen bei der Festlegung einer Migrationsstrategie, mit DataSync der Sie sie umsetzen können.

Inhalt

- [Ermitteln von Datennutzungsmustern](#)
- [Identifizieren der Datenstruktur und des Layouts](#)

- [Dokumentieren von Shares und Ordnern](#)
- [Analysieren von Dateigrößen](#)

Ermitteln von Datennutzungsmustern

- Planen Sie für aktiv genutzte Daten mit häufigen Änderungen mehrere Wellen inkrementeller Übertragungen ein, um eine Unterbrechung des Geschäftsbetriebs zu vermeiden.
- Bei schreibgeschützten Daten, die als archivierend betrachtet werden könnten, müssen Sie möglicherweise keine Wellen einplanen.
- Wenn Sie unterschiedliche Datennutzungsmuster haben, sollten Sie Wellen planen, bei denen diese verschiedenen Datensätze separat migriert werden. Beispielsweise könnten Sie eine Welle für Archivdaten haben, während die restlichen Wellen der Migration aktiver Daten gewidmet sind.

Identifizieren der Datenstruktur und des Layouts

- Stellen Sie fest, ob die Daten nach Zeiträumen (Jahr, Monat, Tag) oder nach anderen Mustern organisiert sind.
- Verwenden Sie diese Organisationsstruktur, um Ihre Migrationswellen zu planen. Beispielsweise könnten Sie während einer Welle Archivdaten für ein Jahr migrieren.

Dokumentieren von Shares und Ordnern

- Erstellen Sie eine Bestandsaufnahme der Freigaben und Ordner (einschließlich der Anzahl der Dateien oder Objekte für jede Datei).
- Identifizieren Sie Shares und Ordner mit aktiven Datensätzen. Diese erfordern möglicherweise inkrementelle Übertragungen während der Migration.
- Überprüfen Sie die [DataSync Kontingente](#). Dies kann Ihnen bei der Planung helfen, wie Sie Ihren Datensatz bei der Konfiguration partitionieren möchten DataSync.

Analysieren von Dateigrößen

- Erwarten Sie bei Übertragungen mit größeren Dateien (MB oder GB) einen höheren Datendurchsatz als bei kleineren Dateien (KB).

- Wenn Sie mit vielen kleineren Dateien arbeiten, müssen Sie mit mehr Metadatenoperationen auf Ihrem Speichersystem und einem geringeren Datendurchsatz rechnen. DataSync führt diese Operationen aus, wenn Sie Ihre Quell- und Zielspeicherorte vergleichen und verifizieren.

Identifizierung der Speicheranforderungen

Um einen kompatiblen AWS Speicherservice für die Migration Ihrer Daten auszuwählen, müssen Sie die Eigenschaften und die Leistung Ihres Quellspeichersystems bewerten.

Diese Informationen können Ihnen auch bei der [Planung Ihrer Übertragungen](#) helfen, um die Auswirkungen auf den Geschäftsbetrieb während der Migration so gering wie möglich zu halten.

Inhalt

- [Bestimmung der Unterstützung für den Quellspeicher](#)
- [Überprüfung der Anforderungen an die Aufbewahrung von Metadaten](#)
- [Erfassung von Leistungsmetriken aus dem Quellspeicher](#)
- [Auswahl eines AWS Zielspeicherdienstes](#)

Bestimmung der Unterstützung für den Quellspeicher

DataSync kann mit einer Vielzahl von Speichersystemen arbeiten, die den Zugriff über NFS-, SMB-, HDFS- und S3-kompatible Objektspeicherclients ermöglichen.

Wenn Sie von einem anderen Cloud-Speicher migrieren, stellen Sie sicher, dass dieser mit diesem DataSync Anbieter funktioniert. Eine Liste der unterstützten Quellverzeichnis finden Sie unter [Mit wem kann ich meine Daten übertragen AWS DataSync?](#)

Überprüfung der Anforderungen an die Aufbewahrung von Metadaten

DataSync kann Ihre Datei- oder Objektmetadaten während einer Übertragung beibehalten. Wie Ihre Metadaten erhalten bleiben, hängt von Ihren Übertragungsorten ab und davon, ob diese Speicherorte ähnliche Arten von Metadaten verwenden.

DataSync benötigt in einigen Fällen zusätzliche Berechtigungen zur Aufbewahrung von Dateimetadaten, wie z. B. diskretionäre NTFS-Zugriffslisten (DACLs).

Weitere Informationen finden Sie unter [Verstehen, wie DataSync mit Datei- und Objektmetadaten umgegangen wird.](#)

Erfassung von Leistungsmetriken aus dem Quellspeicher

Messen Sie die Ausgangs-IOPS und den Festplattendurchsatz bei durchschnittlichen und Spitzenauslastungen für Ihren Quellspeicher. Die Übertragung von Daten erhöht den I/O Mehraufwand sowohl für Ihre Quell- als auch für Ihre Zielspeichersysteme.

Vergleichen Sie diese Leistungsdaten mit den Spezifikationen Ihres Speichersystems, um die verfügbaren Leistungsressourcen zu ermitteln.

Auswahl eines AWS Zielspeicherdienstes

Zu diesem Zeitpunkt haben Sie vielleicht eine Vorstellung davon, welcher AWS Speicherdienst für Ihre Daten sinnvoll ist. Wenn nicht, sind Datennutzungsmuster und Speicherleistung einige Bereiche, die Sie bei Ihrer Entscheidung berücksichtigen sollten. Sie könnten beispielsweise Amazon S3 in Betracht ziehen, wenn Sie über Archivdaten verfügen, und Amazon FSx oder Amazon EFS für aktive Daten.

Informationen zur Auswahl des richtigen objekt- oder dateibasierten Speichers für Ihre Daten finden Sie unter [Auswahl eines AWS Speicherdienstes](#).

Ermitteln der Netzwerkanforderungen

Um Ihre Daten mit zu migrieren DataSync, müssen Sie Netzwerkverbindungen zwischen Ihrem Quellspeicher, Ihrem Agenten und herstellen AWS. Außerdem müssen Sie genügend Netzwerkbandbreite und Infrastruktur einplanen.

Ermitteln Sie gemeinsam mit Ihren Netzwerktechnikern und Speicheradministratoren die folgenden Netzwerkanforderungen.

Inhalt

- [Bewertung Ihrer verfügbaren Netzwerkbandbreite](#)
- [Erwägen Sie Optionen für die Verbindung Ihres Netzwerks mit AWS](#)
- [Auswahl eines Dienstendpunkts für die Agentenkommunikation](#)
- [Planung einer ausreichenden Netzwerkinfrastruktur](#)

Bewertung Ihrer verfügbaren Netzwerkbandbreite

Ihre verfügbare Netzwerkbandbreite wirkt sich auf Ihre Übertragungsgeschwindigkeiten und die Gesamt migrationszeit aus. Gehen Sie wie folgt vor, wenn Sie von einem lokalen Speichersystem aus Daten übertragen:

- Ermitteln Sie gemeinsam mit Ihrem Netzwerkteam die durchschnittliche und maximale Bandbreitennutzung.
- Identifizieren Sie Zeitfenster, in denen Sie Daten übertragen können, und vermeiden Sie so Störungen des täglichen Betriebs. Auf diese Weise erhalten Sie Informationen darüber, wann Ihre Migrationswellen und Umstellungen stattfinden.

Sie können kontrollieren, wie viel Bandbreite DataSync verwendet wird. Weitere Informationen finden Sie unter [Legen Sie Bandbreitenlimits für Ihre Aufgabe fest AWS DataSync](#).

Da Übertragungen von anderen Cloud-Speichern in der Regel über das öffentliche Internet erfolgen, gibt es bei diesen Übertragungen in der Regel weniger Bandbreitenbeschränkungen und Überlegungen.

Erwägen Sie Optionen für die Verbindung Ihres Netzwerks mit AWS

Erwägen Sie die folgenden Optionen, um die Netzwerkkonnektivität für Ihre DataSync Übertragung herzustellen:

- Direct Connect- Sehen Sie sich die [Architektur- und Routing-Beispiele](#) für die Verwendung von Direct Connect mit an DataSync. Sie können die Direct Connect-Aktivitäten mit [Amazon](#) überwachen CloudWatch.
- VPN — [AWS Site-to-Site VPN](#) bietet einen Durchsatz von bis zu 1,25 Gbit/s pro Tunnel.
- Öffentliches Internet — Informationen zur Netzwerknutzung erhalten Sie von Ihrem Internetdienstanbieter.

Auswahl eines Dienstendpunkts für die Agentenkommunikation

DataSync Agenten verwenden [Dienstendpunkte](#), um mit dem DataSync Dienst zu kommunizieren. Welchen Endpunkttyp Sie verwenden, hängt davon ab, wie Sie sich mit Ihrem Netzwerk verbinden AWS.

Planung einer ausreichenden Netzwerkinfrastruktur

Generiert und verwaltet für jede Übertragungsaufgabe, die Sie erstellen, DataSync automatisch die Netzwerkinfrastruktur für Ihre Datenübertragungen. Diese Infrastruktur wird als Netzwerkschnittstellen oder Elastic Network Interfaces bezeichnet. Dabei handelt es sich um logische Netzwerkkomponenten in einer Amazon Virtual Private Cloud (VPC), die virtuelle Netzwerkkarten darstellen. Weitere Informationen finden Sie im [EC2 Amazon-Benutzerhandbuch](#).

Jede Netzwerkschnittstelle verwendet eine einzelne IP-Adresse in Ihrem Ziel-VPC-Subnetz. Gehen Sie wie folgt vor, um sicherzustellen, dass Sie über eine ausreichende Netzwerkinfrastruktur für Ihre Migration verfügen:

- Notieren Sie sich die Anzahl der [Netzwerkschnittstellen](#), die für Ihren DataSync Zielstandort erstellt werden.
- Stellen Sie sicher, dass Ihr Subnetz über genügend IP-Adressen für Ihre DataSync Aufgaben verfügt. Für eine Aufgabe, die einen Agenten verwendet, sind beispielsweise vier IP-Adressen erforderlich. Wenn Sie vier Aufgaben für Ihre Migration erstellen, bedeutet das, dass Sie 16 verfügbare IP-Adressen in Ihrem Subnetz benötigen.

Durchführung eines DataSync Machbarkeitsnachweises

Durch die Durchführung eines Machbarkeitsnachweises (POC) AWS DataSync können Sie die folgenden Aspekte Ihrer Datenmigrationsplanung überprüfen:

- Überprüfen Sie die Netzwerkkonnektivität zwischen Quell- und Zielstandorten.
- Überprüfen Sie Ihre anfängliche DataSync Aufgabenkonfiguration.
- Messen Sie die Leistung der Datenübertragung.
- Schätzen Sie die Migrationszeitpläne ab.
- Definieren Sie gemeinsam mit den wichtigsten Akteuren, die an der Migration arbeiten, Erfolgskriterien.

Erste Schritte mit Ihrem Machbarkeitsnachweis

1. Erstellen Sie Ihren DataSync Agenten:
 1. [Stellen Sie Ihren Agenten](#) bereit.
 2. [Wählen Sie einen Service-Endpunkt](#) für Ihren Agenten.
 3. [Aktivieren Sie Ihren Agenten](#).
 4. [Überprüfen Sie die Netzwerkverbindungen Ihres Agenten](#).
2. Wählen Sie eine kleine Teilmenge von Daten aus, die die Daten darstellt, die Sie migrieren.

Wenn Ihr Quellspeicher beispielsweise eine Mischung aus großen und kleinen Dateien enthält, sollte die Teilmenge der Daten, die Sie in Ihrem POC übertragen, dies widerspiegeln. Auf

diese Weise erhalten Sie einen ersten Überblick über die Leistung der Speichersysteme, Ihres Netzwerks und. DataSync

3. Erstellen Sie einen DataSync Quellspeicherort für Ihr [lokales](#) oder ein [anderes Cloud-Speichersystem](#).
4. Erstellen Sie einen DataSync Zielort für Ihren [AWS Speicherdienst](#).
5. [Erstellen Sie eine DataSync Übertragungsaufgabe](#) mit einem [Filter](#), der nur Ihre Datenteilmenge überträgt.
6. [Starte deine DataSync Aufgabe](#).
7. Erfassen Sie Kennzahlen zur Übertragungsleistung, indem Sie Folgendes überwachen:
 - Der Daten- und Dateidurchsatz Ihrer Aufgabenausführung. Sie können dies über die DataSync Konsole oder die [DescribeTaskExecution](#) Operation tun. Wenn Sie diese Metriken verwenden `DescribeTaskExecution`, berechnen Sie sie wie folgt:
 - Datendurchsatz: Dividieren `BytesWritten` durch `TransferDuration`
 - Dateidurchsatz: Dividiere `FilesTransferred` durch `TransferDuration`
 - Nutzung des Quell- und Zielspeichers. Arbeiten Sie eng mit Ihren Speicheradministratoren zusammen, um diese Informationen zu erhalten.
 - Netzwerknutzung.
8. Überprüfen Sie die übertragenen Daten an Ihrem Zielort:
 - Überprüfen Sie Ihre CloudWatch Protokolle auf Fehler bei der Ausführung von Aufgaben.
 - Stellen Sie sicher, dass die Berechtigungen und Metadaten am Zielspeicherort erhalten bleiben.
 - Stellen Sie sicher, dass Anwendungen und Benutzer wie erwartet auf Zieldaten zugreifen können.
 - Beheben Sie alle Probleme, auf die Sie stoßen. Weitere Informationen finden Sie unter [AWS DataSync Probleme beheben](#).
9. Führen Sie Ihre Aufgabe noch einige Male aus, um eine Vorstellung davon DataSync zu bekommen, wie lange die Vorbereitung, Übertragung und Überprüfung Ihrer Daten dauert. (Weitere Informationen finden Sie unter [Status der Aufgabenausführung](#).)

Wenn Sie eine Aufgabe mehrmals ausführen, führt sie DataSync standardmäßig eine inkrementelle Übertragung durch und kopiert nur die Daten, die sich gegenüber der vorherigen Aufgabenausführung geändert haben.

Bei inkrementellen Übertragungen wird die Übertragungszeit wahrscheinlich kürzer sein, aber Ihre Übertragung DataSync wird immer auf die gleiche Weise vorbereitet, indem Sie Ihre Standorte scannen und vergleichen, um herauszufinden, was übertragen werden soll. Anhand dieser Vorbereitungszeiten können Sie die [Umstellungsfristen für Ihre Migration abschätzen](#).

10. Falls erforderlich, aktualisieren Sie Ihren Migrationsplan auf der Grundlage dessen, was Sie während des POC gelernt haben.

Schätzung der Migrationszeitpläne

Anhand der Informationen, die Sie bis jetzt gesammelt haben, können Sie abschätzen, wie lange die Migration dauern wird. AWS DataSync

Schätzung der Zeitpläne für die Datenübertragung

Anhand der folgenden Informationen, die Sie bei der Erfassung der Migrationsanforderungen und Ihres DataSync Machbarkeitsnachweises (POC) gesammelt haben, können Sie abschätzen, wie lange die Übertragung Ihrer Daten dauert DataSync :

- Ihre [verfügbare Netzwerkbandbreite](#)
- Kennzahlen zur Quell- und Zielspeichernutzung
- Leistungskennzahlen aus Ihrem [DataSync POC](#)

Um einen Zeitplan für die Datenübertragung abzuschätzen

1. Vergleichen Sie den Daten- und Dateidurchsatz Ihres POC mit Ihrer verfügbaren Netzwerkbandbreite.
2. Wenn Ihr Durchsatz niedriger als Ihre verfügbare Bandbreite ist (z. B. 300 MiB/s für einen Durchsatz mit 10 Gbit/s Netzwerkbandbreite), sollten Sie erwägen, Ihren Datensatz in mehrere Aufgaben zu partitionieren, um die Bandbreitennutzung zu maximieren.

DataSync bietet einige Optionen zur Partitionierung Ihres Datensatzes. Weitere Informationen finden Sie unter [Beschleunigen Sie Ihre Migration durch Datenpartitionierung](#).

3. Berechnen Sie anhand der folgenden Formel, die eine theoretische Mindestübertragungszeit ergibt, wie viele Tage eine Übertragung dauert:

$$(\text{DATA\_SIZE} * 8 \text{ bits per byte}) / (\text{CIRCUIT} * \text{NETWORK\_UTILIZATION percentage} * 3600 \text{ seconds per hour} * \text{AVAILABLE\_HOURS}) = \text{Number of days}$$

Wenn Sie diese Formel verwenden, ersetzen Sie Folgendes durch Ihre eigenen Werte:

- DATA_SIZE: Die Datenmenge, die Sie migrieren (ausgedrückt in Byte).
- CIRCUIT: Ihre verfügbare Netzwerkbandbreite (ausgedrückt in Bit pro Sekunde).
- NETWORK_UTILIZATION: Wie viel Prozent Ihres Netzwerks werden genutzt?
- AVAILABLE_HOURS: Die Anzahl der an jedem Tag verfügbaren Betriebsstunden.

Sie würden beispielsweise eine Migration mit 100 TB Daten, einer Internetverbindung von 1 Gbit/s, einer Netzauslastung von 80 Prozent und einer Verfügbarkeit von 24 Stunden pro Tag wie folgt berechnen:

$$(100,000,000,000,000 \text{ bytes} * 8) / (1,000,000,000 \text{ bps} * 0.80 * 3600 * 24) = 11.57 \text{ days}$$

In diesem Fall würde die Migration fast 12 Tage dauern, bevor die realen Bedingungen berücksichtigt werden.

4. Passen Sie Ihre berechnete Übertragungsdauer an die realen Bedingungen an:

- Schwankungen der Netzwerkleistung
- Schwankungen der Speicherleistung
- Ausfallzeiten zwischen den Migrationswellen

Schätzung der Umstellungsfristen

Wenn Sie aktive Datensätze migrieren, benötigen Sie wahrscheinlich Umstellungen, um den Geschäftsbetrieb nicht zu stören.

Unterschätzen Sie nicht, wie lange Umstellungen dauern. Bei großen Migrationen ist es nicht ungewöhnlich, dass Umstellungsaktivitäten bis zu 30 Prozent Ihrer gesamten Migrationszeit in Anspruch nehmen.

1. Prüfen Sie, ob Sie Umstellungen in Wellen durchführen müssen, um die Datenmenge zu reduzieren, die nach inkrementellen Änderungen gescannt wird.

Eine Strategie hierfür ist das Überschneiden von Datensätzen, die Sie auf der Grundlage von Freigaben, Ordern oder Speichersystemen partitionieren.

2. Prüfen Sie, wie lange es in der Regel gedauert hat, Ihre Daten während des POC vorzubereiten, DataSync zu übertragen und zu verifizieren.

Beachten Sie insbesondere die Vorbereitungsdauer Ihrer Aufgabenausführungen. Um diese Informationen zu finden, führen Sie den [DescribeTaskExecution](#) Vorgang aus und überprüfen Sie dann den Wert [PrepareDuration](#) für die Dauer (in Millisekunden).

3. Schätzen Sie ab, wie lange eine Umstellung dauern könnte, indem Sie das Zeitdelta zwischen parallel Aufgaben messen.

Weitere Informationen zu parallel Aufgaben finden Sie unter [Beschleunigen Sie Ihre Migration durch Datenpartitionierung](#).

4. Verwenden Sie Ihre Umsatzschätzung, um Ihre Umstellungen zu planen. Dabei handelt es sich im Wesentlichen um Wartungsfenster, in denen Ihre Quelldaten nicht geändert werden können.

Nächste Schritte

Nachdem Sie Ihre Zeitpläne geschätzt haben, können Sie mit der Implementierung Ihrer Migration beginnen.

Phase 2: Implementierung Ihrer Migration großer Datenmengen

Mit den Informationen, die Sie bei der Planung gesammelt haben, können Sie mit der Migration AWS DataSync auf Ihr neues Speichersystem beginnen. Falls Sie dies noch nicht getan haben, empfehlen wir Ihnen, die [Ressourcen zu AWS Prescriptive Guidance für umfangreiche](#) Migrationen zu lesen.

Themen

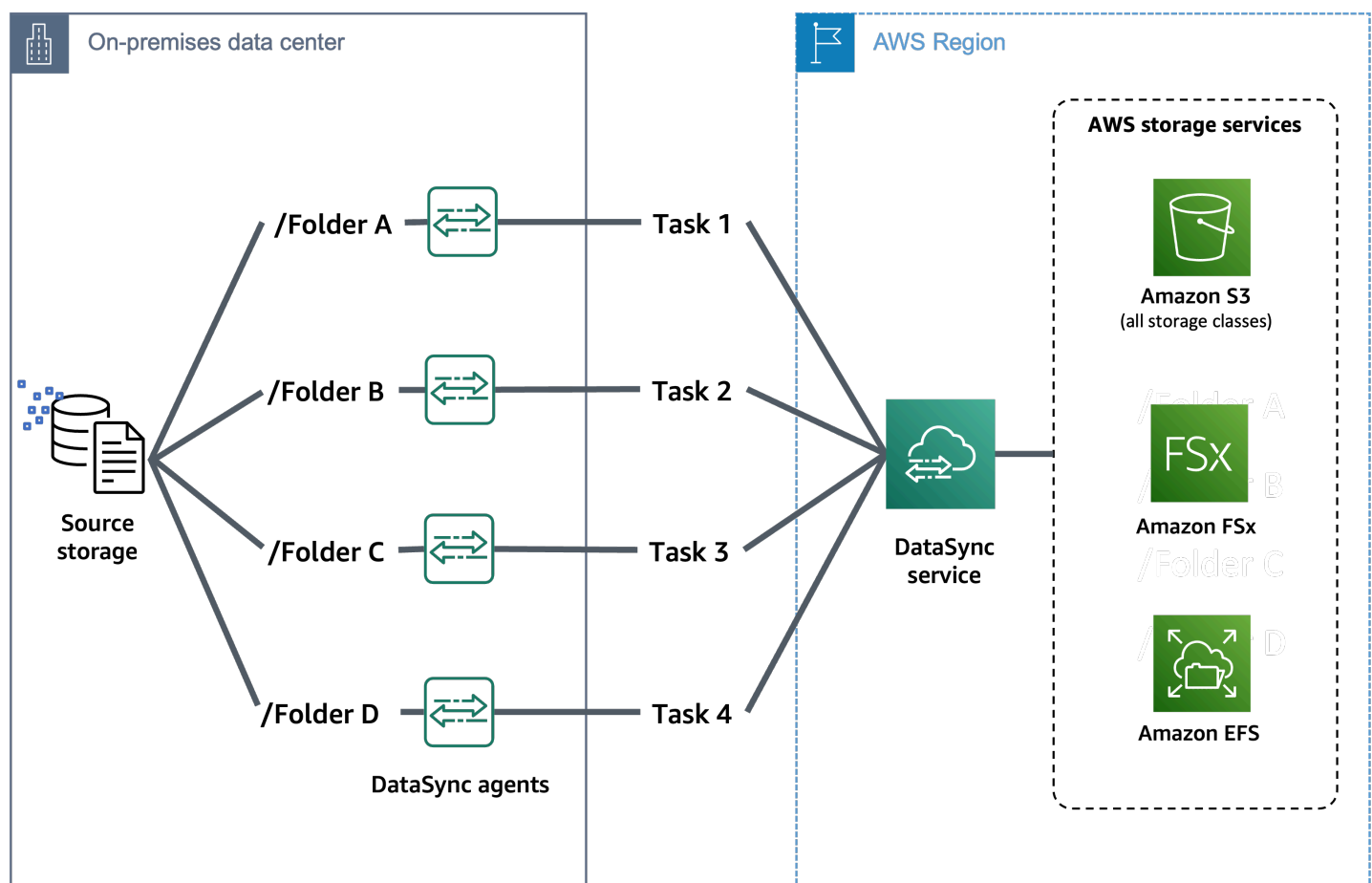
- [Beschleunigen Sie Ihre Migration durch Datenpartitionierung](#)
- [Ausführen Ihrer DataSync Übertragungsaufgaben](#)
- [Überwachen Sie Ihre Übertragungen](#)

Beschleunigen Sie Ihre Migration durch Datenpartitionierung

Bei einer großen Migration empfehlen wir, Ihren Datensatz mit mehreren DataSync Aufgaben zu partitionieren. Durch die Partitionierung Ihrer Quelldaten auf mehrere Aufgaben (und möglicherweise Agenten) können Sie Ihre Übertragungen parallelisieren und den Migrationszeitraum verkürzen.

Die Partitionierung hilft Ihnen auch dabei, die DataSync [Kontingente](#) einzuhalten, und vereinfacht die Überwachung und das Debuggen Ihrer Aufgaben.

Das folgende Diagramm zeigt, wie Sie mehrere DataSync Aufgaben und Agenten verwenden können, um Daten aus demselben Quellspeicherort zu übertragen. In diesem Szenario konzentriert sich jede Aufgabe auf einen bestimmten Ordner am Quellspeicherort. Weitere Informationen und Beispiele zu diesen Ansätzen finden Sie unter [So beschleunigen Sie Ihre Datenübertragungen mit AWS DataSync Scale-out-Architekturen](#).



Partitionierung Ihres Datensatzes nach Ordner oder Präfix

Wenn Sie Ihren DataSync Quellspeicherort erstellen, können Sie einen Ordner, ein Verzeichnis oder ein Präfix angeben, aus dem DataSync gelesen wird. Wenn Sie beispielsweise eine Dateifreigabe mit

Verzeichnissen der obersten Ebene migrieren, können Sie mehrere Speicherorte erstellen, die einen anderen Verzeichnispfad angeben. Sie können diese Speicherorte dann verwenden, um während Ihrer Migration mehrere DataSync Aufgaben auszuführen.

Partitionierung Ihres Datensatzes mit Filtern

Sie können [Filter](#) anwenden, um Daten aus Ihrem Quellstandort in eine Übertragung ein- oder auszuschließen. Im Kontext einer großen Migration können Filter Ihnen helfen, Aufgaben auf bestimmte Teile Ihres Datensatzes einzugrenzen.

Wenn Sie beispielsweise Archivdaten migrieren, die nach Jahren organisiert sind, können Sie einen Einschlussfilter erstellen, der für ein bestimmtes Jahr oder mehrere Jahre geeignet ist. Sie können den Filter auch bei jeder Ausführung der Aufgabe so ändern, dass er einem anderen Jahr entspricht.

Partitionieren Sie Ihren Datensatz mit Manifesten

Ein [Manifest](#) ist eine Liste von Dateien oder Objekten, die Sie übertragen DataSync möchten. Bei einem Manifest müssen Sie DataSync nicht alles in einem Quellverzeichnis lesen, um zu bestimmen, was übertragen werden soll.

Sie können Manifeste aus den Beständen Ihres Quellspeichers oder mithilfe ereignisgesteuerter Methoden erstellen (siehe z. B. [Implementierung AWS DataSync mit Hunderten von Millionen von Objekten](#)). Sie können auch bei jedem Start einer Aufgabe ein anderes Manifest verwenden, sodass Sie verschiedene Datensätze mit derselben Aufgabe übertragen können.

Ausführen Ihrer DataSync Übertragungsaufgaben

Während jeder Ihrer Migrationswellen folgt Ihre Datenübertragung in der Regel demselben allgemeinen Prozess:

1. Führen Sie eine erste vollständige Übertragung Ihrer Daten durch.
2. Überprüfen Sie die Daten im Ziel.
3. Führen Sie inkrementelle Übertragungen für alle Daten durch, die sich seit der ersten Übertragung möglicherweise geändert haben.
4. Verlagern Sie den Betrieb an Ihrem Zielort.
5. Überprüfen Sie die Ergebnisse der Umstellung.

Ihre Aufgaben ausführen

Wahrscheinlich müssen Sie Ihre DataSync Übertragungsaufgaben während der Geschäftszeiten ausführen, um Ihre Gesamtmigrationszeit zu minimieren. In diesen Situationen ist es üblich, zunächst eine vollständige Übertragung durchzuführen, gefolgt von inkrementellen Übertragungen, bei denen Änderungen von Benutzern und Anwendungen an Ihrem Quellstandort berücksichtigt werden.

Um Netzwerkprobleme während der Geschäftszeiten zu vermeiden, können Sie die Bandbreite begrenzen, die Ihre Aufgaben beanspruchen. Weitere Informationen finden Sie unter [Legen Sie Bandbreitenlimits für Ihre Aufgabe fest AWS DataSync](#).

1. Führen Sie eine erste vollständige Übertragung durch:
 - a. [Starten Sie Ihre DataSync Aufgabe](#) (oder Aufgaben, wenn Sie Aufgaben parallel ausführen).
 - b. Überwachen Sie den Fortschritt und die Leistung Ihrer Aufgabenausführungen.
 - c. Stellen Sie sicher, dass Ihre Daten erwartungsgemäß übertragen wurden (z. B. werden Dateimetadaten beibehalten).
2. Führen Sie inkrementelle Übertragungen durch:
 - a. [Planen Sie Ihre Aufgaben](#) so, dass sie regelmäßig ausgeführt werden.
 - b. Überwachen Sie Ihre Aufgabenausführungen und beheben Sie etwaige Fehler.

Durchführung einer Umstellung

Nach Ihren ersten und schrittweisen Übertragungen können Sie mit der Umstellung des Betriebs auf Ihren Zielstandort beginnen.

1. Starten Sie das geplante Wartungsfenster.
2. Aktualisieren Sie Ihr Quellspeichersystem so, dass es nur für Anwendungen und Benutzer lesbar ist.
3. Führen Sie letzte inkrementelle Übertragungen durch, um die verbleibenden Deltas zwischen Ihren Quell- und Zielorten zu kopieren.
4. Führen Sie eine gründliche Datenvalidierung durch (z. B. durch Überprüfung von CloudWatch Protokollen und [Aufgabenberichten](#)).
5. Stellen Sie Ihre Anwendungen und Benutzer auf die neue Umgebung Ihres Zielstandorts um.
6. Testen Sie die Anwendungsfunktionalität und stellen Sie sicher, dass Benutzer auf Daten an Ihrem Zielstandort zugreifen können.

7. Vereinbaren Sie ein Treffen mit den Migrationsteams, um den Transfer im Nachhinein zu besprechen. Stellen Sie die folgenden Beispielfragen zur Sondierung:
 - War die Umstellung erfolgreich? Falls nicht, was war das Problem?
 - Haben wir die gesamte verfügbare Bandbreite genutzt?
 - Wurden der Quell- und Zielspeicher voll ausgelastet?
 - Können wir mit zusätzlichen Aufgaben mehr Datendurchsatz erzielen?
 - Müssen wir ein längeres Wartungsfenster einplanen?
8. Falls erforderlich, aktualisieren Sie Ihren Migrationsplan, bevor Sie mit der nächsten Welle beginnen.

Überwachen Sie Ihre Übertragungen

AWS DataSync bietet verschiedene Überwachungsoptionen, mit denen Sie Ihre Übertragung validieren und debuggen können.

Überwachen Sie Ihre Übertragungen mit Metriken CloudWatch

Sie können benutzerdefinierte CloudWatch Dashboards mit Metriken aus Ihren DataSync Aufgabenausführungen erstellen. Weitere Informationen finden Sie unter [Überwachung von Datenübertragungen mit CloudWatch Amazon-Metriken](#).

Überwachen Sie Ihre Übertragungen mit Aufgabenberichten

Wenn Sie Millionen von Dateien oder Objekten übertragen, sollten Sie die Verwendung von Aufgabenberichten in Betracht ziehen. Aufgabenberichte enthalten detaillierte Informationen darüber, welche DataSync Versuche während der Ausführung einer Aufgabe zu übertragen, zu überspringen, zu überprüfen und zu löschen sind. Weitere Informationen finden Sie unter [Überwachen Sie Ihre Datenübertragungen mit Aufgabenberichten](#).

Sie können Ihre Aufgabenberichte auch mithilfe von AWS Diensten wie AWS Glue Amazon Athena und Amazon Quick Suite visualisieren. Weitere Informationen finden Sie im [AWS Storage-Blog](#).

Überwachen Sie Ihre Übertragungen mit CloudWatch Logs

Wir empfehlen Ihnen, Ihre Aufgabe mindestens so zu konfigurieren, dass grundlegende Informationen und Übertragungsfehler protokolliert werden. Weitere Informationen finden Sie unter [Überwachung von Datenübertragungen mit Amazon CloudWatch Logs](#).

AWS DataSync API

Zusätzlich zur AWS-Managementkonsole und AWS CLI können Sie die AWS DataSync API zur Konfiguration und Verwaltung DataSync mit dem verwenden [AWS SDKs](#).

Themen

- [Aktionen](#)
- [Datentypen](#)
- [Häufige Fehler](#)
- [Geläufige Parameter](#)

Aktionen

Folgende Aktionen werden unterstützt:

- [CancelTaskExecution](#)
- [CreateAgent](#)
- [CreateLocationAzureBlob](#)
- [CreateLocationEfs](#)
- [CreateLocationFsxLustre](#)
- [CreateLocationFsxOntap](#)
- [CreateLocationFsxOpenZfs](#)
- [CreateLocationFsxWindows](#)
- [CreateLocationHdfs](#)
- [CreateLocationNfs](#)
- [CreateLocationObjectStorage](#)
- [CreateLocationS3](#)
- [CreateLocationSmb](#)
- [CreateTask](#)
- [DeleteAgent](#)
- [DeleteLocation](#)
- [DeleteTask](#)

- [DescribeAgent](#)
- [DescribeLocationAzureBlob](#)
- [DescribeLocationEfs](#)
- [DescribeLocationFsxLustre](#)
- [DescribeLocationFsxOntap](#)
- [DescribeLocationFsxOpenZfs](#)
- [DescribeLocationFsxWindows](#)
- [DescribeLocationHdfs](#)
- [DescribeLocationNfs](#)
- [DescribeLocationObjectStorage](#)
- [DescribeLocationS3](#)
- [DescribeLocationSmb](#)
- [DescribeTask](#)
- [DescribeTaskExecution](#)
- [ListAgents](#)
- [ListLocations](#)
- [ListTagsForResource](#)
- [ListTaskExecutions](#)
- [ListTasks](#)
- [StartTaskExecution](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateAgent](#)
- [UpdateLocationAzureBlob](#)
- [UpdateLocationEfs](#)
- [UpdateLocationFsxLustre](#)
- [UpdateLocationFsxOntap](#)
- [UpdateLocationFsxOpenZfs](#)
- [UpdateLocationFsxWindows](#)
- [UpdateLocationHdfs](#)

- [UpdateLocationNfs](#)
- [UpdateLocationObjectStorage](#)
- [UpdateLocationS3](#)
- [UpdateLocationSmb](#)
- [UpdateTask](#)
- [UpdateTaskExecution](#)

CancelTaskExecution

Stoppt die Ausführung einer AWS DataSync Aufgabe, die gerade läuft. Die Übertragung einiger Dateien wird abrupt unterbrochen. Dateiinhalte, die an das Ziel übertragen werden, sind möglicherweise unvollständig oder stimmen nicht mit den Quelldateien überein.

Wenn Sie jedoch eine neue Aufgabenausführung mit derselben Aufgabe starten und warten, bis sie abgeschlossen ist, ist der Dateiinhalt auf dem Ziel vollständig und konsistent. Dies gilt für andere unerwartete Fehler, die die Ausführung einer Aufgabe unterbrechen. In all diesen Fällen schließt die Übertragung DataSync erfolgreich ab, wenn Sie die nächste Aufgabenausführung starten.

Anforderungssyntax

```
{  
  "TaskExecutionArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

TaskExecutionArn

Der Amazon-Ressourcenname (ARN) der Aufgabenausführung, die gestoppt werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateAgent

Aktiviert einen AWS DataSync Agenten, den Sie in Ihrer Speicherumgebung bereitstellen. Der Aktivierungsprozess verknüpft den Agenten mit Ihrem AWS-Konto.

Falls Sie noch keinen Agenten eingesetzt haben, finden Sie weitere Informationen unter [Benötige ich einen DataSync Agenten?](#)

Anforderungssyntax

```
{
  "ActivationKey": "string",
  "AgentName": "string",
  "SecurityGroupArns": [ "string" ],
  "SubnetArns": [ "string" ],
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "VpcEndpointId": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[ActivationKey](#)

Gibt den Aktivierungsschlüssel Ihres DataSync Agenten an. Wenn Sie keinen Aktivierungsschlüssel haben, finden Sie weitere Informationen unter [Aktivierung Ihres Agenten](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 29.

Pattern: `[A-Z0-9]{5}(-[A-Z0-9]{5}){4}`

Erforderlich: Ja

AgentName

Gibt einen Namen für Ihren Agenten an. Wir empfehlen, einen Namen anzugeben, an den Sie sich erinnern können.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Erforderlich: Nein

SecurityGroupArns

Gibt den Amazon-Ressourcennamen (ARN) der Sicherheitsgruppe an, die den Datenverkehr zwischen Ihrem Agenten und dem VPC-Serviceendpunkt zulässt. Sie können nur einen ARN angeben.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Feste Anzahl von 1 Element.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erforderlich: Nein

SubnetArns

Gibt den ARN des Subnetzes an, in dem sich Ihr VPC-Dienstendpunkt befindet. Sie können nur einen ARN angeben.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Feste Anzahl von 1 Element.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:subnet/subnet-[a-f0-9]+$`

Erforderlich: Nein

Tags

Gibt Labels an, die Ihnen helfen, Ihre AWS Ressourcen zu kategorisieren, zu filtern und nach ihnen zu suchen. Wir empfehlen, mindestens ein Tag für Ihren Agenten zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

VpcEndpointId

Gibt die ID des [VPC-Dienstendpunkts](#) an, den Sie verwenden. Eine VPC-Endpoint-ID sieht beispielsweise so `vpce-01234d5aff67890e1` aus.

Important

Der von Ihnen verwendete VPC-Dienstendpunkt muss den DataSync Dienstnamen enthalten (z. B. `com.amazonaws.us-east-2.datasync`).

Typ: Zeichenfolge

Pattern: `^vpce-[0-9a-f]{17}$`

Erforderlich: Nein

Antwortsyntax

```
{
  "AgentArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AgentArn

Der ARN des Agenten, den Sie gerade aktiviert haben. Verwenden Sie den [ListAgents](#) Vorgang, um eine Liste der Agenten in Ihrem Land AWS-Konto zurückzugeben AWS-Region.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Im folgenden Beispiel wird ein DataSync Agent aktiviert.

```
{
  "ActivationKey": "AAAAA-1AAAA-BB1CC-33333-EEEEEE",
  "AgentName": "MyAgent",
  "Tags": [{
    "Key": "Job",
    "Value": "TransferJob-1"
  }]
}
```

```
}
```

Beispielantwort

Die Antwort gibt den ARN des aktivierten Agenten zurück.

```
{  
  "AgentArn": "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44baca3"  
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationAzureBlob

Erstellt einen Übertragungsort für einen Microsoft Azure Blob Storage-Container. AWS DataSync kann diesen Speicherort als Übertragungsquelle oder -ziel verwenden. Sie können Übertragungen mit oder ohne einen [DataSync Agenten](#) durchführen, der eine Verbindung zu Ihrem Container herstellt.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, [wie auf Azure Blob Storage DataSync zugegriffen](#) wird und wie mit [Zugriffsebenen](#) und [Blobtypen](#) gearbeitet wird.

Anforderungssyntax

```
{
  "AccessTier": "string",
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlobType": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "ContainerUrl": "string",
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "SasConfiguration": {
    "Token": "string"
  },
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccessTier

Gibt die Zugriffsebene an, in die Ihre Objekte oder Dateien übertragen werden sollen. Dies gilt nur, wenn der Standort als Übertragungsziel verwendet wird. Weitere Informationen finden Sie unter [Zugriffsebenen](#).

Typ: Zeichenfolge

Zulässige Werte: HOT | COOL | ARCHIVE

Erforderlich: Nein

AgentArns

(Optional) Gibt den Amazon-Ressourcennamen (ARN) des DataSync Agenten an, der eine Verbindung mit Ihrem Azure Blob Storage-Container herstellen kann. Wenn Sie eine cloudübergreifende Übertragung ohne Agenten einrichten, müssen Sie für diesen Parameter keinen Wert angeben.

Sie können mehr als einen Agenten angeben. Weitere Informationen finden Sie unter [Mehrere Agenten für Ihre Übertragung verwenden](#).

Note

Stellen Sie sicher, dass Sie diesen Parameter korrekt konfigurieren, wenn Sie Ihren Speicherort zum ersten Mal erstellen. Nachdem Sie einen Speicherort erstellt haben, können Sie keine Agenten mehr hinzufügen oder daraus entfernen.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

AuthenticationType

Gibt die Authentifizierungsmethode an, die für den Zugriff auf Ihren Azure Blob Storage DataSync verwendet wird. DataSync kann mithilfe einer Shared Access Signature (SAS) auf Blob-Speicher zugreifen.

Typ: Zeichenfolge

Zulässige Werte: SAS | NONE

Erforderlich: Ja

BlobType

Gibt den Blobtyp an, den Ihre Objekte oder Dateien haben sollen, wenn sie in Azure Blob Storage übertragen werden. Unterstützt derzeit DataSync nur das Verschieben von Daten in Azure Blob Storage als Blockblobs. Weitere Informationen zu Blobtypen finden Sie in der [Azure Blob Storage](#)-Dokumentation.

Typ: Zeichenfolge

Zulässige Werte: BLOCK

Erforderlich: Nein

CmkSecretConfig

Gibt Konfigurationsinformationen für ein vom Kunden DataSync verwaltetes Geheimnis an, zu dem auch das Authentifizierungstoken gehört, das für den Zugriff auf einen bestimmten AzureBlob Speicherort DataSync verwendet wird. AWS KMS key

Wenn Sie diesen Parameter als Teil einer `CreateLocationAzureBlob` Anfrage angeben, geben Sie nur den KMS-Schlüssel ARN an. DataSync verwendet diesen KMS-Schlüssel zusammen mit dem von Ihnen angegebenen `AuthentifizierungstokenSasConfiguration`, um ein DataSync verwaltetes Geheimnis zum Speichern der Standortzugriffsanmeldeinformationen zu erstellen.

Stellen Sie sicher, dass dieser Benutzer berechtigt DataSync ist, auf den von Ihnen angegebenen KMS-Schlüssel zuzugreifen.

Note

Sie können entweder `CmkSecretConfig (mitSasConfiguration)` oder `CustomSecretConfig (ohneSasConfiguration)` verwenden, um

Anmeldeinformationen für eine `CreateLocationAzureBlob` Anfrage bereitzustellen. Geben Sie nicht beide Parameter für dieselbe Anfrage an.

Typ: [CmkSecretConfig](#) Objekt

Erforderlich: Nein

[ContainerUrl](#)

Gibt die URL des Azure Blob Storage-Containers an, der an Ihrer Übertragung beteiligt ist.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 325.

Pattern: `^https:\\\\[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}\\/[a-z0-9](-?[a-z0-9]){2,62}$`

Erforderlich: Ja

[CustomSecretConfig](#)

Gibt Konfigurationsinformationen für einen vom Kunden verwalteten Secrets Manager Secret an, bei dem das Authentifizierungstoken für einen AzureBlob Speicherort im Klartext in Secrets Manager gespeichert wird. Diese Konfiguration umfasst den geheimen ARN und den ARN für eine IAM-Rolle, die Zugriff auf den geheimen Schlüssel ermöglicht.

Note

Sie können entweder `CmkSecretConfig` (mit `SasConfiguration`) oder `CustomSecretConfig` (ohne `SasConfiguration`) Anmeldeinformationen für eine `CreateLocationAzureBlob` Anfrage angeben. Geben Sie nicht beide Parameter für dieselbe Anfrage an.

Typ: [CustomSecretConfig](#) Objekt

Erforderlich: Nein

[SasConfiguration](#)

Gibt die SAS-Konfiguration an, die DataSync den Zugriff auf Ihren Azure Blob Storage ermöglicht.

Note

Wenn Sie mithilfe von `CmkSecretConfig` oder ein Authentifizierungstoken bereitstellen `SasConfiguration`, aber keine geheimen Konfigurationsdetails angeben `CustomSecretConfig`, DataSync speichert das Token dann unter Verwendung des Secrets Managers Secret Ihres AWS Kontos.

Typ: [AzureBlobSasConfiguration](#) Objekt

Erforderlich: Nein

Subdirectory

Gibt Pfadsegmente an, wenn Sie Ihre Übertragung auf ein virtuelles Verzeichnis in Ihrem Container beschränken möchten (z. B. `/my/images`).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 1 024.

Pattern: `^[\\p{L}\\p{M}\\p{Z}\\p{S}\\p{N}\\p{P}\\p{C}]*$`

Erforderlich: Nein

Tags

Gibt Bezeichnungen an, mit denen Sie Ihre AWS -Ressourcen kategorisieren, filtern und suchen können. Wir empfehlen, mindestens ein Namensschild für Ihren Übertragungsort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{
  "LocationArn": "string"
}
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

LocationArn

Der ARN des Azure Blob Storage-Übertragungsorts, den Sie erstellt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationEfs

Erstellt einen Übertragungsort für ein Amazon EFS-Dateisystem. AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie DataSync [auf Amazon EFS-Dateisysteme zugegriffen](#) wird.

Anforderungssyntax

```
{
  "AccessPointArn": "string",
  "Ec2Config": {
    "SecurityGroupArns": [ "string" ],
    "SubnetArn": "string"
  },
  "EfsFileSystemArn": "string",
  "FileSystemAccessRoleArn": "string",
  "InTransitEncryption": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AccessPointArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des Access Points an, der zum Mounten Ihres Amazon EFS-Dateisystems DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugreifen auf eingeschränkte Dateisysteme](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

Erforderlich: Nein

[Ec2Config](#)

Gibt das Subnetz und die Sicherheitsgruppen an, die für die Verbindung zu einem der [Mount-Ziele](#) Ihres Amazon EFS-Dateisystems DataSync verwendet werden.

Typ: [Ec2Config](#) Objekt

Erforderlich: Ja

[EfsFileSystemArn](#)

Gibt den ARN für Ihr Amazon EFS-Dateisystem an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]{8,40}$`

Erforderlich: Ja

[FileSystemAccessRoleArn](#)

Gibt eine AWS Identity and Access Management (IAM-) Rolle an, die DataSync den Zugriff auf Ihr Amazon EFS-Dateisystem ermöglicht.

Informationen zum Erstellen dieser Rolle finden Sie unter [Eine DataSync IAM-Rolle für den Dateisystemzugriff erstellen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Erforderlich: Nein

InTransitEncryption

Gibt an, ob Sie DataSync die Transport Layer Security (TLS) 1.2-Verschlüsselung verwenden möchten, wenn Daten zu oder von Ihrem Amazon EFS-Dateisystem übertragen werden.

Wenn Sie einen Zugriffspunkt mit `AccessPointArn` oder eine IAM-Rolle mit `FileSystemAccessRoleArn` angeben, müssen Sie diesen Parameter auf `TLS1_2` setzen.

Typ: Zeichenfolge

Zulässige Werte: `NONE` | `TLS1_2`

Erforderlich: Nein

Subdirectory

Gibt einen Mount-Pfad für Ihr Amazon-EFS-Dateisystem an. Hier werden Daten in Ihrem Dateisystem DataSync gelesen oder geschrieben (je nachdem, ob es sich um einen Quell- oder Zielspeicherort handelt).

DataSync Verwendet standardmäßig das Stammverzeichnis (oder den [Zugriffspunkt](#), falls Sie eines mit `angebenAccessPointArn`). Sie können Unterverzeichnisse auch mit Schrägstrichen einbeziehen (z. B. `/path/to/folder`).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Erforderlich: Nein

Tags

Gibt Schlüssel-Wert-Paar an, das für ein Tag steht, das Sie der Ressource hinzufügen möchten. Der Wert kann auch eine leere Zeichenfolge sein. Dieser Wert hilft Ihnen, Ressourcen zu verwalten, zu filtern und zu suchen. Wir empfehlen Ihnen, für Ihren Speicherort ein Namens-Tag anzulegen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{  
  "LocationArn": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der Amazon-Ressourcenname (ARN) des Amazon EFS-Dateisystemspeicherorts, den Sie erstellen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Im folgenden Beispiel wird ein Speicherort für ein Amazon EFS-Dateisystem erstellt.

```
{
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:11122233344:subnet/
subnet-1234567890abcdef1",
    "SecurityGroupArns": [
      "arn:aws:ec2:us-east-2:11122233344:security-group/sg-1234567890abcdef2"
    ]
  },
  "EfsFileSystemArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:file-system/
fs-021345abcdef6789",
  "Subdirectory": "/mount/path",
  "Tags": [{
    "Key": "Name",
    "Value": "ElasticFileSystem-1"
  }]
}
```

Beispielanforderung: Erstellen eines Speicherorts für ein eingeschränktes Amazon EFS-Dateisystem

Im folgenden Beispiel wird ein Speicherort für ein Amazon EFS-Dateisystem mit eingeschränktem Zugriff erstellt. In einem solchen Szenario müssen Sie möglicherweise Werte für `AccessPointArnFileSystemAccessRoleArn`, und `InTransitEncryption` in Ihrer Anfrage angeben.

```
{
  "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:access-point/
fsap-1234567890abcdef0",
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/
subnet-1234567890abcdef1",
```

```

    "SecurityGroupArns": [
        "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
    ],
    "FileSystemAccessRoleArn": "arn:aws:iam::111222333444:role/AwsDataSyncFullAccessNew",
    "InTransitEncryption": "TLS1_2",
    "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-abcdef01234567890",
    "LocationUri": "efs://us-east-2.fs-021345abcdef6789/",
    "Subdirectory": "/mount/path",
    "Tags": [{
        "Key": "Name",
        "Value": "ElasticFileSystem-1"
    }]
}

```

Beispielantwort

Eine Antwort gibt den Standort-ARN des Amazon EFS-Dateisystems zurück.

```

{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-12abcdef012345678"
}

```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)

- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationFsxLustre

Erstellt einen Übertragungsort für ein Amazon FSx for Lustre-Dateisystem. AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie DataSync [auf Lustre-Dateisysteme zugegriffen FSx](#) wird.

Anforderungssyntax

```
{
  "FsxFilesystemArn": "string",
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[FsxFilesystemArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des FSx for Lustre-Dateisystems an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

Erforderlich: Ja

SecurityGroupArns

Gibt die Amazon-Ressourcennamen (ARNs) von bis zu fünf Sicherheitsgruppen an, die den Zugriff auf Ihr FSx for Lustre-Dateisystem ermöglichen.

Die Sicherheitsgruppen müssen auf die Ports des Dateisystems zugreifen können. Das Dateisystem muss auch den Zugriff von den Sicherheitsgruppen aus ermöglichen. Informationen zum Dateisystemzugriff finden Sie im [Amazon FSx for Lustre-Benutzerhandbuch](#).

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erforderlich: Ja

Subdirectory

Gibt einen Bereitstellungspfad für Ihr FSx for Lustre-Dateisystem an. Der Pfad kann Unterverzeichnisse enthalten.

Wenn der Speicherort als Quelle verwendet wird, DataSync liest Daten aus dem Mount-Pfad. Wenn der Speicherort als Ziel verwendet wird, werden Daten in den Bereitstellungspfad DataSync geschrieben. Wenn Sie diesen Parameter nicht angeben, DataSync verwendet das Stammverzeichnis des Dateisystems (/).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\+\.\^(\)\$\p{Zs}]+$`

Erforderlich: Nein

Tags

Gibt Bezeichnungen an, mit denen Sie Ihre AWS -Ressourcen kategorisieren, filtern und suchen können. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{  
  "LocationArn": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der Amazon-Ressourcenname (ARN) des FSx for Lustre-Dateisystemspeicherorts, den Sie erstellt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationFsxOntap

Erstellt einen Übertragungsort für ein Amazon FSx for NetApp ONTAP-Dateisystem. AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie [auf ONTAP-Dateisysteme DataSync zugegriffen FSx](#) wird.

Anforderungssyntax

```
{
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "SecurityGroupArns": [ "string" ],
  "StorageVirtualMachineArn": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Protocol

Gibt das Datenübertragungsprotokoll an, das für den Zugriff auf Ihr FSx Amazon-Dateisystem AWS DataSync verwendet wird.

Typ: [FsxProtocol](#) Objekt

Erforderlich: Ja

SecurityGroupArns

Gibt die EC2 Amazon-Sicherheitsgruppen an, die den Zugriff auf das bevorzugte Subnetz Ihres Dateisystems ermöglichen.

Die Sicherheitsgruppen müssen ausgehenden Datenverkehr an den folgenden Ports zulassen (abhängig vom verwendeten Protokoll):

- Netzwerk-Dateisystem (NFS): TCP-Ports 111, 635 und 2 049
- Server Message Block (SMB): TCP-Port 445

Die Sicherheitsgruppen Ihres Dateisystems müssen auch eingehenden Datenverkehr über dieselben Ports zulassen.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erforderlich: Ja

StorageVirtualMachineArn

Gibt den ARN der Storage Virtual Machine (SVM, virtuelle Speichermaschine) in Ihrem Dateisystem an, in die Sie Daten kopieren wollen.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 162.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

Erforderlich: Ja

Subdirectory

Gibt den Pfad zur Dateifreigabe auf der SVM an, zu der oder von der Sie Daten übertragen möchten.

Sie können einen Knotenpfad (auch als Mount-Punkt bezeichnet), einen Qtree-Pfad (für NFS-Dateifreigaben) oder einen Share-Namen (für SMB-Dateifreigaben) angeben. Ihr Mount-Pfad könnte zum Beispiel `/vol1`, `/vol1/tree1` oder `/share1` sein.

Note

Geben Sie keinen Verbindungspfad im Stammvolume der SVM an. Weitere Informationen finden Sie unter [Verwaltung FSx virtueller ONTAP-Speichermaschinen](#) im Amazon FSx for NetApp ONTAP-Benutzerhandbuch.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Erforderlich: Nein

Tags

Gibt Bezeichnungen an, mit denen Sie Ihre AWS -Ressourcen kategorisieren, filtern und suchen können. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{
  "LocationArn": "string"
}
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

LocationArn

Gibt den ARN des Speicherorts FSx für das Dateisystem für ONTAP an, den Sie erstellen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationFsxOpenZfs

Erstellt einen Übertragungsort für ein Amazon FSx for OpenZFS-Dateisystem. AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie DataSync [Zugriffe auf FSx OpenZFS-Dateisysteme funktionieren](#).

Note

Anforderungsparameter, die sich auf beziehen, SMB werden von dem Vorgang nicht unterstützt. CreateLocationFsxOpenZfs

Anforderungssyntax

```
{
  "FsxFilesystemArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

```
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[FsxFilesystemArn](#)

Der Amazon-Ressourcenname (ARN) des FSx Dateisystems für OpenZFS.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

Erforderlich: Ja

[Protocol](#)

Der Protokolltyp, der für den Zugriff auf Ihr Dateisystem AWS DataSync verwendet wird.

Typ: [FsxProtocol](#) Objekt

Erforderlich: Ja

[SecurityGroupArns](#)

Die Sicherheitsgruppen, die zur Konfiguration ARNs des Dateisystems FSx für OpenZFS verwendet werden.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erforderlich: Ja

[Subdirectory](#)

Ein Unterverzeichnis im Pfad des Speicherorts, das mit beginnen muss. /fsx DataSync verwendet dieses Unterverzeichnis zum Lesen oder Schreiben von Daten (je nachdem, ob es sich bei dem Dateisystem um einen Quell- oder Zielspeicherort handelt).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[^\u0000\u0085\u2028\u2029\r\n]{1,4096}$`

Erforderlich: Nein

[Tags](#)

Das Schlüssel-Wert-Paar, das für ein Tag steht, das Sie der Ressource hinzufügen möchten. Der Wert kann auch eine leere Zeichenfolge sein. Dieser Wert hilft Ihnen, Ressourcen zu verwalten, zu filtern und zu suchen. Wir empfehlen Ihnen, für Ihren Speicherort ein Namens-Tag anzulegen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{
  "LocationArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der ARN des Speicherorts FSx für das OpenZFS-Dateisystem, den Sie erstellt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im Dienst ein Fehler auftritt. AWS DataSync

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)

- [AWS SDK for Ruby V3](#)

CreateLocationFsxWindows

Erstellt einen Übertragungsort für ein Dateisystem von Amazon FSx für Windows File Server. AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie DataSync [Zugriffe auf FSx Windows File Server-Dateisysteme funktionieren](#).

Anforderungssyntax

```
{
  "Domain": "string",
  "FsxFilesystemArn": "string",
  "Password": "string",
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "User": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[Domain](#)

Gibt den Namen der Windows-Domäne an, zu der das Dateisystem FSx für Windows File Server gehört.

Wenn Sie mehrere Active Directory-Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen Dateisystem hergestellt wird.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Erforderlich: Nein

FsxFilesystemArn

Gibt den Amazon-Ressourcennamen (ARN) für das Dateisystem FSx für Windows File Server an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

Erforderlich: Ja

Password

Gibt das Passwort des Benutzers an, der berechtigt ist, die Dateien, Ordner und Dateimetadaten in Ihrem Dateisystem FSx für Windows File Server bereitzustellen und darauf zuzugreifen.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^\.{0,104}$`

Erforderlich: Ja

SecurityGroupArns

Gibt die ARNs EC2 Amazon-Sicherheitsgruppen an, die den Zugriff auf das bevorzugte Subnetz Ihres Dateisystems ermöglichen.

Die von Ihnen angegebenen Sicherheitsgruppen müssen in der Lage sein, mit den Sicherheitsgruppen Ihres Dateisystems zu kommunizieren. Informationen zur Konfiguration von Sicherheitsgruppen für den Dateisystemzugriff finden Sie im [Amazon FSx for Windows File Server-Benutzerhandbuch](#).

Note

Wenn Sie eine Sicherheitsgruppe wählen, die keine internen Verbindungen zulässt, gehen Sie wie folgt vor:

- Konfigurieren Sie die Sicherheitsgruppe so, dass sie mit sich selbst kommunizieren kann.
- Wählen Sie eine andere Sicherheitsgruppe, die mit der Sicherheitsgruppe des Mount-Ziels kommunizieren kann.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erforderlich: Ja

Subdirectory

Gibt einen Mount-Pfad für Ihr Dateisystem mithilfe von Schrägstrichen an. Hier werden Daten DataSync gelesen oder geschrieben (je nachdem, ob es sich um einen Quell- oder Zielort handelt).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\+\.\^(\)\$\p{Zs}]+$`

Erforderlich: Nein

Tags

Gibt Bezeichnungen an, mit denen Sie Ihre AWS -Ressourcen kategorisieren, filtern und suchen können. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

User

Gibt den Benutzer an, der berechtigt ist, die Dateien, Ordner und Dateimetadaten in Ihrem Dateisystem FSx für Windows File Server bereitzustellen und darauf zuzugreifen.

Informationen zur Auswahl eines Benutzers mit der richtigen Zugriffsebene für Ihre Übertragung finden Sie unter [Erforderliche Berechtigungen](#) FSx für Windows-Dateiserverstandorte.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\\x22\\x5B\\x5D\\/\\:;|=, +*?\\x3C\\x3E]{1,104}$`

Erforderlich: Ja

Antwortsyntax

```
{
  "LocationArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der ARN des Dateisystemspeicherorts FSx für Windows File Server, den Sie erstellt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationHdfs

Erstellt einen Übertragungsort für ein Hadoop Distributed File System (HDFS). AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie auf DataSync [HDFS-Cluster zugegriffen](#) wird.

Anforderungssyntax

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlockSize": number,
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "KmsKeyProviderUri": "string",
  "NameNodes": [
    {
      "Hostname": "string",
      "Port": number
    }
  ],
  "QopConfiguration": {
    "DataTransferProtection": "string",
    "RpcProtection": "string"
  },
  "ReplicationFactor": number,
  "SimpleUser": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AgentArns](#)

Die Amazon-Ressourcennamen (ARNs) der DataSync Agenten, die eine Verbindung zu Ihrem HDFS-Cluster herstellen können.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Ja

[AuthenticationType](#)

Die Art der Authentifizierung, die verwendet wird, um die Identität des Benutzers zu ermitteln.

Typ: Zeichenfolge

Zulässige Werte: SIMPLE | KERBEROS

Erforderlich: Ja

[BlockSize](#)

Die Größe der Datenblöcke, die in den HDFS-Cluster geschrieben werden sollen. Die Blockgröße muss ein Vielfaches von 512 Bytes sein. Die standardmäßige Blockgröße ist 128 Mebibyte (MiB).

Typ: Ganzzahl

Gültiger Bereich: Mindestwert von 1048576. Der Höchstwert ist 1073741824.

Erforderlich: Nein

KerberosKeytab

Die Kerberos-Schlüsseltabelle (keytab), die Zuweisungen zwischen dem definierten Kerberos-Prinzipal und den verschlüsselten Schlüsseln enthält. Sie können den Keytab aus einer Datei laden, indem Sie die Adresse der Datei angeben.

Note

Dieser Parameter ist erforderlich, wenn KERBEROS für AuthenticationType festgelegt ist.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 65536.

Erforderlich: Nein

KerberosKrb5Conf

Die krb5.conf-Datei, die die Kerberos-Konfigurationsinformationen enthält. Sie können die krb5.conf Datei laden, indem Sie die Adresse der Datei angeben. Wenn Sie das verwenden AWS CLI, führt es die Base64-Kodierung für Sie durch. Andernfalls geben Sie den Base64-codierten Text an.

Note

Dieser Parameter ist erforderlich, wenn KERBEROS für AuthenticationType festgelegt ist.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 131072.

Erforderlich: Nein

KerberosPrincipal

Das Kerberos-Prinzipal mit Zugriff auf die Dateien und Ordner im HDFS-Cluster.

Note

Dieser Parameter ist erforderlich, wenn KERBEROS für AuthenticationType festgelegt ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^.+`

Erforderlich: Nein

KmsKeyProviderUri

Die URI des Key Management Servers (KMS) des HDFS-Clusters.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Pattern: `^kms:\\\\http[s]?@(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9])(;(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9]))*:[0-9]{1,5}\\kms$`

Erforderlich: Nein

NameNodes

Der NameNode , der den HDFS-Namespace verwaltet. Der NameNode führt Operationen wie das Öffnen, Schließen und Umbenennen von Dateien und Verzeichnissen aus. Das NameNode enthält die Informationen zum Zuordnen von Datenblöcken zu. DataNodes Sie können nur einen verwenden NameNode.

Typ: Array von [HdfsNameNode](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element.

Erforderlich: Ja

QopConfiguration

Die Konfiguration der Quality of Protection (QOP, Schutzqualität) legt den Remote Procedure Call (RPC) und die Datenschutzeinstellungen für die Datenübertragung fest, die auf dem Hadoop Distributed File System (HDFS)-Cluster konfiguriert sind. Wenn QopConfiguration nicht angegeben ist, ist PRIVACY der Standardwert für RpcProtection und DataTransferProtection. Wenn Sie RpcProtection oder DataTransferProtection festlegen, nimmt der andere Parameter den gleichen Wert an.

Typ: [QopConfiguration](#) Objekt

Erforderlich: Nein

ReplicationFactor

Die Nummer DataNodes , auf die die Daten repliziert werden sollen, wenn in den HDFS-Cluster geschrieben wird. Standardmäßig werden Daten auf drei repliziert. DataNodes

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Der Maximalwert ist 512.

Erforderlich: Nein

SimpleUser

Der zur Identifizierung des Clients auf dem Host-Betriebssystem verwendete Benutzername.

Note

Dieser Parameter ist erforderlich, wenn SIMPLE für AuthenticationType festgelegt ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[_.A-Za-z0-9][_.A-Za-z0-9]*$`

Erforderlich: Nein

[Subdirectory](#)

Ein Unterverzeichnis im HDFS-Cluster. Dieses Unterverzeichnis wird verwendet, um Daten vom HDFS-Cluster zu lesen oder zu schreiben. Wenn das Unterverzeichnis nicht angegeben ist, ist es standardmäßig `/`.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\+\.\^(\)\$\p{Zs}]+$`

Erforderlich: Nein

[Tags](#)

Das Schlüssel-Wert-Paar, das für das Tag steht, das Sie dem Speicherort hinzufügen möchten. Der Wert kann auch eine leere Zeichenfolge sein. Wir empfehlen, zum Benennen Ihrer Ressourcen Tags zu verwenden.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{  
  "LocationArn": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der ARN des Quell-HDFS-Cluster-Speicherorts, den Sie erstellen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)

- [AWS SDK for Ruby V3](#)

CreateLocationNfs

Erstellt einen Übertragungsort für einen NFS-Dateiserver (Network File System). AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie auf [NFS-Dateiserver DataSync zugegriffen](#) wird.

Anforderungssyntax

```
{
  "MountOptions": {
    "Version": "string"
  },
  "OnPremConfig": {
    "AgentArns": [ "string" ]
  },
  "ServerHostname": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[MountOptions](#)

Gibt die Optionen an, die zum Mounten Ihres NFS-Dateiservers verwendet werden DataSync können.

Typ: [NfsMountOptions](#) Objekt

Erforderlich: Nein

OnPremConfig

Gibt den Amazon-Ressourcennamen (ARN) des DataSync Agenten an, der eine Verbindung zu Ihrem NFS-Dateiserver herstellen kann.

Sie können mehr als einen Agenten angeben. Weitere Informationen finden Sie unter [Mehrere DataSync Agenten verwenden](#).

Typ: [OnPremConfig](#) Objekt

Erforderlich: Ja

ServerHostname

Gibt den DNS-Namen oder die IP-Adresse (IPv4 oder IPv6) des NFS-Dateiservers an, mit dem Ihr DataSync Agent eine Verbindung herstellt.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^(( [a-zA-Z0-9\ - ]*[a-zA-Z0-9])\ . )*( [A-Za-z0-9\ - : ]*[A-Za-z0-9] )$`

Erforderlich: Ja

Subdirectory

Gibt den Exportpfad auf Ihrem NFS-Dateiserver an, den Sie mounten DataSync möchten.

Dieser Pfad (oder ein Unterverzeichnis des Pfads) ist der Ort, an den Daten DataSync übertragen werden oder von diesem Pfad. Informationen zur Konfiguration eines Exports für DataSync finden Sie unter [Zugreifen auf NFS-Dateiserver](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\ -\+\.\^(\)\p{Zs}]+$`

Erforderlich: Ja

Tags

Gibt Beschriftungen an, die Ihnen helfen, Ihre Ressourcen zu kategorisieren, zu filtern und nach ihnen zu AWS suchen. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{  
  "LocationArn": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der ARN des Übertragungsorts, den Sie für Ihren NFS-Dateiserver erstellt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispiel

Im folgenden Beispiel wird ein DataSync Übertragungsort für einen NFS-Dateiserver erstellt.

Beispielanforderung

```
{
  "MountOptions": {
    "Version": : "NFS4_0"
  },
  "OnPremConfig": {
    "AgentArn": [ "arn:aws:datasync:us-east-2:111222333444:agent/
agent-0b0addbeef44b3nfs" ]
  },

  "ServerHostname": "MyServer@amazon.com",
  "Subdirectory": "/MyFolder",
  "Tags": [
    {
      "Key": "Name",
      "Value": "FileSystem-1"
    }
  ]
}
```

Beispiel

Die Antwort gibt den ARN des NFS-Standorts zurück.

Beispielantwort

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
```

```
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationObjectStorage

Erzeugt einen Übertragungsort für ein Objektspeichersystem. AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden. Sie können Übertragungen mit oder ohne einen [DataSyncAgenten durchführen](#).

Bevor Sie beginnen, stellen Sie sicher, dass Sie die [Voraussetzungen](#) für DataSync die Arbeit mit Objektspeichersystemen verstehen.

Anforderungssyntax

```
{
  "AccessKey": "string",
  "AgentArns": [ "string" ],
  "BucketName": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "SecretKey": "string",
  "ServerCertificate": blob,
  "ServerHostname": "string",
  "ServerPort": number,
  "ServerProtocol": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccessKey

Gibt den Zugriffsschlüssel (z. B. einen Benutzernamen) an, wenn Anmeldeinformationen für die Authentifizierung beim Objektspeicher-Server erforderlich sind.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Höchstlänge = 200 Zeichen.

Pattern: `^\.*$`

Erforderlich: Nein

AgentArns

(Optional) Gibt die Amazon-Ressourcennamen (ARNs) der DataSync Agenten an, die eine Verbindung zu Ihrem Objektspeichersystem herstellen können. Wenn Sie eine cloudübergreifende Übertragung ohne Agenten einrichten, müssen Sie für diesen Parameter keinen Wert angeben.

Note

Stellen Sie sicher, dass Sie diesen Parameter korrekt konfigurieren, wenn Sie Ihren Speicherort zum ersten Mal erstellen. Nachdem Sie einen Speicherort erstellt haben, können Sie keine Agenten mehr hinzufügen oder daraus entfernen.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

BucketName

Gibt den Namen des Objektspeicher-Buckets an, der an der Übertragung beteiligt ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 3. Maximale Länge beträgt 63 Zeichen.

Pattern: `^[a-zA-Z0-9_\-\.\\(\)\$\p{Zs}]+$`

Erforderlich: Ja

[CmkSecretConfig](#)

Gibt Konfigurationsinformationen für ein vom Kunden DataSync AWS KMS key verwaltetes Geheimnis an, zu dem auch der Schlüssel gehört `SecretKey`, der für den Zugriff auf einen bestimmten Objektspeicherort DataSync verwendet wird.

Wenn Sie diesen Parameter als Teil einer `CreateLocationObjectStorage` Anfrage angeben, geben Sie nur den KMS-Schlüssel ARN an. DataSync verwendet diesen KMS-Schlüssel zusammen mit dem Wert, den Sie für den `SecretKey` Parameter angeben, um ein DataSync verwaltetes Geheimnis zum Speichern der Anmeldeinformationen für den Standortzugriff zu erstellen.

Stellen Sie sicher, dass dieser Benutzer berechtigt DataSync ist, auf den von Ihnen angegebenen KMS-Schlüssel zuzugreifen.

Note

Sie können entweder `CmkSecretConfig` (mit `SecretKey`) oder `CustomSecretConfig` (ohne `SecretKey`) verwenden, um Anmeldeinformationen für eine `CreateLocationObjectStorage` Anfrage bereitzustellen. Geben Sie nicht beide Parameter für dieselbe Anfrage an.

Typ: [CmkSecretConfig](#) Objekt

Erforderlich: Nein

[CustomSecretConfig](#)

Gibt Konfigurationsinformationen für ein vom Kunden verwaltetes Secrets Manager-Geheimnis an, bei dem der geheime Schlüssel für einen bestimmten Objektspeicherort im Klartext in Secrets Manager gespeichert wird. Diese Konfiguration umfasst den geheimen ARN und den ARN für eine IAM-Rolle, die Zugriff auf den geheimen Schlüssel ermöglicht.

Note

Sie können entweder `CmkSecretConfig` (mit `SecretKey`) oder `CustomSecretConfig` (ohne `SecretKey`) Anmeldeinformationen für eine `CreateLocationObjectStorage` Anfrage angeben. Geben Sie nicht beide Parameter für dieselbe Anfrage an.

Typ: [CustomSecretConfig](#) Objekt

Erforderlich: Nein

[SecretKey](#)

Gibt den geheimen Schlüssel (z. B. ein Passwort) an, wenn Anmeldeinformationen für die Authentifizierung beim Objektspeicher-Server erforderlich sind.

Note

Wenn Sie mithilfe von `CmkSecretConfig` oder ein Geheimnis angeben `SecretKey`, aber keine geheimen Konfigurationsdetails angeben `CustomSecretConfig`, DataSync speichert das Token unter Verwendung des Secrets Manager Manager-Geheimnisses Ihres AWS Kontos.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Höchstlänge = 200 Zeichen.

Pattern: `^\.*$`

Erforderlich: Nein

[ServerCertificate](#)

Gibt eine Zertifikatskette für DataSync die Authentifizierung bei Ihrem Objektspeichersystem an, falls das System eine private oder selbstsignierte Zertifizierungsstelle (CA) verwendet. Sie müssen eine einzelne `.pem` Datei mit einer vollständigen Zertifikatskette angeben (z. B. `file:///home/user/.ssh/object_storage_certificates.pem`).

Die Zertifikatskette könnte Folgendes beinhalten:

- Das Zertifikat des Objektspeichersystems

- Alle Zwischenzertifikate (falls vorhanden)
- Das Stammzertifikat der signierenden Zertifizierungsstelle

Sie können Ihre Zertifikate zu einer .pem Datei zusammenfügen (die vor der Base64-Kodierung bis zu 32768 Byte groß sein kann). Mit dem folgenden `cat` Beispielbefehl wird eine `object_storage_certificates.pem` Datei erstellt, die drei Zertifikate enthält:

```
cat object_server_certificate.pem intermediate_certificate.pem  
ca_root_certificate.pem > object_storage_certificates.pem
```

Um diesen Parameter zu verwenden, konfigurieren Sie `ServerProtocol` auf `HTTPS`.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 32768.

Erforderlich: Nein

ServerHostname

Gibt den Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Objektspeicherservers an, mit dem Ihr DataSync Agent eine Verbindung herstellt.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^(( [a-zA-Z0-9\ - ]*[a-zA-Z0-9] )\ . )*( [A-Za-z0-9\ - : ]*[A-Za-z0-9] )$`

Erforderlich: Ja

ServerPort

Gibt den Port an, an dem Ihr Objektspeicher-Server eingehenden Netzwerkverkehr annimmt (z. B. Port 443).

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Der Höchstwert ist 65536.

Erforderlich: Nein

ServerProtocol

Gibt das Protokoll an, das Ihr Objektspeicher-Server für die Kommunikation verwendet. Wenn nichts angegeben ist, lautet der Standardwert `HTTPS`.

Typ: Zeichenfolge

Zulässige Werte: HTTPS | HTTP

Erforderlich: Nein

[Subdirectory](#)

Gibt das Objekt-Präfix für Ihren Objektspeicher-Server an. Wenn es sich um einen Quellspeicherort handelt, werden DataSync nur Objekte mit diesem Präfix kopiert. Wenn es sich um einen Zielort handelt, werden alle Objekte mit diesem Präfix DataSync geschrieben.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Erforderlich: Nein

[Tags](#)

Gibt Schlüssel-Wert-Paar an, das für ein Tag steht, das Sie der Ressource hinzufügen möchten. Mithilfe von Tags können Sie Ihre Ressourcen verwalten, filtern und suchen. Wir empfehlen, ein Namensschild für Ihren Standort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{  
  "LocationArn": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

LocationArn

Gibt den ARN des Objekt-Storage-Systemspeicherorts an, den Sie erstellen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationS3

Erstellt einen Übertragungsort für einen Amazon S3 S3-Bucket. AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Important

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Themen gelesen haben:

- [Überlegungen zur Speicherklasse bei Amazon S3 S3-Standorten](#)
- [Bewertung der Kosten für S3-Anfragen bei der Verwendung DataSync](#)

Weitere Informationen finden Sie unter [Konfiguration von Übertragungen mit Amazon S3](#).

Anforderungssyntax

```
{
  "AgentArns": [ "string" ],
  "S3BucketArn": "string",
  "S3Config": {
    "BucketAccessRoleArn": "string"
  },
  "S3StorageClass": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AgentArns

(Nur Amazon S3 bei Outposts) Gibt den Amazon-Ressourcennamen (ARN) des DataSync Agenten in Ihrem Outpost an.

Weitere Informationen finden Sie unter [Bereitstellen Ihres DataSync Agenten auf AWS Outposts](#).

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

S3BucketArn

Gibt den ARN des S3-Buckets an, den Sie als Speicherort verwenden möchten. (Wenn Sie Ihre DataSync Aufgabe später erstellen, geben Sie an, ob es sich bei diesem Speicherort um eine Übertragungsquelle oder ein Übertragungsziel handelt.)

Wenn sich Ihr S3-Bucket auf einer AWS Outposts Ressource befindet, müssen Sie einen Amazon S3 S3-Zugriffspunkt angeben. Weitere Informationen finden Sie unter [Verwaltung des Datenzugriffs mit Amazon S3 S3-Zugriffspunkten](#) im Amazon S3 S3-Benutzerhandbuch.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 268.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:[a-z\-\0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3-outposts:[a-z\-\0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-.]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_{1,255}$`

Erforderlich: Ja

S3Config

Gibt den Amazon-Ressourcennamen (ARN) der AWS Identity and Access Management (IAM) - Rolle an, die für den Zugriff auf Ihren S3-Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [DataSync Zugriff auf S3-Buckets bereitstellen](#).

Typ: [S3Config](#) Objekt

Erforderlich: Ja

[S3StorageClass](#)

Gibt die Speicherklasse an, die Ihre Objekte verwenden sollen, wenn Amazon S3 ein Übertragungsziel ist.

Für Buckets in ist AWS-Regionen die Speicherklasse standardmäßig auf eingestellt. STANDARD
Bei aktivierten Buckets ist AWS Outposts die Speicherklasse standardmäßig auf. OUTPOSTS

Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#).

Typ: Zeichenfolge

Zulässige Werte: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING |
GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Erforderlich: Nein

[Subdirectory](#)

Gibt ein Präfix im S3-Bucket an, das DataSync Lese- oder Schreibvorgänge vornimmt (je nachdem, ob es sich bei dem Bucket um einen Quell- oder Zielspeicherort handelt).

Note

DataSync kann keine Objekte mit einem Präfix übertragen, das mit einem Schrägstrich (/) beginnt oder /. / Muster einschließt//. / ./ Beispiel:

- /photos
- photos//2006/January
- photos/./2006/February
- photos/./2006/March

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Erforderlich: Nein

Tags

Gibt Beschriftungen an, die Ihnen helfen, Ihre Ressourcen zu kategorisieren, zu filtern und nach ihnen zu AWS suchen. Wir empfehlen, mindestens ein Namensschild für Ihren Transferort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

Antwortsyntax

```
{
  "LocationArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der ARN des S3-Standorts, den Sie erstellt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateLocationSmb

Erstellt einen Übertragungsort für einen SMB-Dateiserver (Server Message Block). AWS DataSync kann diesen Speicherort als Quelle oder Ziel für die Übertragung von Daten verwenden.

Bevor Sie beginnen, stellen Sie sicher, dass Sie wissen, wie auf SMB-Dateiserver DataSync zugegriffen wird. Weitere Informationen finden Sie unter [Bereitstellen des DataSync Zugriffs auf SMB-Dateiserver](#).

Anforderungssyntax

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "DnsIpAddresses": [ "string" ],
  "Domain": "string",
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "MountOptions": {
    "Version": "string"
  },
  "Password": "string",
  "ServerHostname": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "User": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AgentArns](#)

Gibt den DataSync Agenten (oder die Agenten) an, der eine Verbindung zu Ihrem SMB-Dateiserver herstellen kann. Sie geben einen Agenten anhand seines Amazon-Ressourcennamens (ARN) an.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Ja

[AuthenticationType](#)

Gibt das Authentifizierungsprotokoll an, das für die Verbindung mit Ihrem SMB-Dateiserver DataSync verwendet wird. DataSync unterstützt NTLM (Standard) und KERBEROS Authentifizierung.

Weitere Informationen finden Sie unter [Bereitstellen des DataSync Zugriffs auf SMB-Dateiserver](#).

Typ: Zeichenfolge

Zulässige Werte: NTLM | KERBEROS

Erforderlich: Nein

[CmkSecretConfig](#)

Gibt Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis an, entweder ein Password oder KerberosKeytab (für NTLM (Standard-) bzw. KERBEROS Authentifizierungstypen), das für den Zugriff auf einen bestimmten SMB-Speicherort mit einem vom Kunden verwalteten SMB-Speicherort DataSync verwendet wird. AWS KMS key

Wenn Sie diesen Parameter als Teil einer `CreateLocationSmbRequest` Anfrage angeben, geben Sie nur den KMS-Schlüssel ARN an. DataSync verwendet diesen KMS-Schlüssel zusammen mit dem Password oder, den KerberosKeytab Sie angeben, um ein DataSync verwaltetes Geheimnis zum Speichern der Standortzugriffsanmeldeinformationen zu erstellen.

Stellen Sie sicher, dass dieser Benutzer berechtigt DataSync ist, auf den von Ihnen angegebenen KMS-Schlüssel zuzugreifen.

 Note

Sie können entweder `CmkSecretConfig` (mit entweder Password oder `KerberosKeytab`) oder `CustomSecretConfig` (ohne Password und `KerberosKeytab`) verwenden, um Anmeldeinformationen für eine `CreateLocationSmbRequest` Anfrage anzugeben. Geben Sie nicht `CmkSecretConfig` sowohl als auch `CustomSecretConfig` Parameter für dieselbe Anfrage an.

Typ: [CmkSecretConfig](#) Objekt

Erforderlich: Nein

[CustomSecretConfig](#)

Gibt Konfigurationsinformationen für einen vom Kunden verwalteten Secrets Manager Secret an, bei dem die Anmeldeinformationen für den SMB-Speicherort in Secrets Manager als Klartext (`fürPassword`) oder binär (`fürKerberosKeytab`) gespeichert werden. Diese Konfiguration umfasst den geheimen ARN und den ARN für eine IAM-Rolle, die Zugriff auf den geheimen Schlüssel ermöglicht.

 Note

Sie können entweder `CmkSecretConfig` (mit `SasConfiguration`) oder `CustomSecretConfig` (ohne `SasConfiguration`) Anmeldeinformationen für eine `CreateLocationSmbRequest` Anfrage angeben. Geben Sie nicht beide Parameter für dieselbe Anfrage an.

Typ: [CustomSecretConfig](#) Objekt

Erforderlich: Nein

DnsIpAddresses

Gibt die IPv6 Adressen IPv4 oder für die DNS-Server an, zu denen Ihr SMB-Dateiserver gehört. Dieser Parameter gilt nur, wenn er auf KERBEROS gesetzt AuthenticationType ist.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen SMB-Dateiserver hergestellt wird.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Maximale Anzahl von 2 Elementen.

Längenbeschränkungen: Minimale Länge beträgt 7 Zeichen. Die maximale Länge beträgt 39.

Pattern: \A((25[0-5]|2[0-4]\d|[0-1]?[0-9]?[0-9])\.((25[0-5]|2[0-4]\d|[0-1]?[0-9]?[0-9])\d)){3}|([0-9a-fA-F]{1,4}:){7,7}([0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:([0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:(:[0-9a-fA-F]{1,4}){1,6}))\z

Erforderlich: Nein

Domain

Gibt den Windows-Domain-Namen an, zu dem SMB-Dateiserver gehört. Dieser Parameter gilt nur, wenn er auf gesetzt AuthenticationType istNTLM.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen Dateiserver hergestellt wird.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: ^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}\$

Erforderlich: Nein

KerberosKeytab

Gibt Ihre Kerberos-Schlüsseltabellendatei (Keytab) an, die Zuordnungen zwischen Ihrem Kerberos-Prinzipal und den Verschlüsselungsschlüsseln enthält.

Um Fehler bei der Ausführung von Aufgaben zu vermeiden, stellen Sie sicher, dass der Kerberos-Prinzipal, den Sie zum Erstellen der Keytab-Datei verwenden, genau dem entspricht, wofür Sie es angegeben haben. `KerberosPrincipal`

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 65536.

Erforderlich: Nein

KerberosKrb5Conf

Gibt eine Kerberos-Konfigurationsdatei (`krb5.conf`) an, die Ihre Kerberos-Realm-Konfiguration definiert.

Die Datei muss base64-codiert sein. Wenn Sie das verwenden AWS CLI, ist die Kodierung für Sie erledigt.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 131072.

Erforderlich: Nein

KerberosPrincipal

Gibt einen Kerberos-Prinzipal an. Dabei handelt es sich um eine Identität in Ihrem Kerberos-Bereich, die berechtigt ist, auf die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver zuzugreifen.

Ein Kerberos-Prinzipal könnte wie folgt aussehen. `HOST/kerberosuser@MYDOMAIN.ORG`

Bei Prinzipalnamen wird Groß- und Kleinschreibung beachtet. Ihre DataSync Aufgabenausführung schlägt fehl, wenn der Prinzipal, den Sie für diesen Parameter angeben, nicht exakt dem Prinzipal entspricht, den Sie zum Erstellen der Keytab-Datei verwenden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^\.+`

Erforderlich: Nein

MountOptions

Gibt die Version des SMB-Protokolls an, das für den Zugriff auf Ihren SMB-Dateiserver DataSync verwendet wird.

Typ: [SmbMountOptions](#) Objekt

Erforderlich: Nein

Password

Gibt das Kennwort des Benutzers an, der Ihren SMB-Dateiserver bereitstellen kann und über Zugriffsrechte auf die Dateien und Ordner verfügt, die an Ihrer Übertragung beteiligt sind. Dieser Parameter gilt nur, wenn er auf NTLM gesetzt `AuthenticationType` ist.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^\.{0,104}`

Erforderlich: Nein

ServerHostname

Gibt den Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des SMB-Dateiservers an, mit dem Ihr DataSync Agent eine Verbindung herstellt.

Note

Wenn Sie die Kerberos-Authentifizierung verwenden, müssen Sie einen Domänennamen angeben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^(( [a-zA-Z0-9\-\ ]*[a-zA-Z0-9])\.\.)*([A-Za-z0-9\-\ :]*[A-Za-z0-9])$`

Erforderlich: Ja

Subdirectory

Gibt den Namen der von Ihrem SMB-Dateiserver exportierten Freigabe an, auf der Daten gelesen oder geschrieben DataSync werden. Sie können ein Unterverzeichnis in den Freigabepfad aufnehmen (z. B. /path/to/subdirectory). Stellen Sie sicher, dass andere SMB-Clients in Ihrem Netzwerk diesen Pfad ebenfalls bereitstellen können.

Um alle Daten im Unterverzeichnis zu kopieren, DataSync müssen Sie in der Lage sein, die SMB-Freigabe zu mounten und auf alle zugehörigen Daten zuzugreifen. Weitere Informationen finden Sie unter [DataSync Zugriff auf SMB-Dateiserver bereitstellen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\+\.\^(\)\$\\p{Zs}]+$`

Erforderlich: Ja

Tags

Gibt Bezeichnungen an, mit denen Sie Ihre AWS -Ressourcen kategorisieren, filtern und suchen können. Wir empfehlen, zumindest ein Namensschild für Ihren Standort zu erstellen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

User

Gibt den Benutzer an, der die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver bereitstellen und darauf zugreifen kann. Dieser Parameter gilt nur, wenn er auf NTLM gesetzt AuthenticationType ist.

Informationen zur Auswahl eines Benutzers mit der richtigen Zugriffsebene für Ihre Übertragung finden Sie unter [DataSync Zugriff auf SMB-Dateiserver bereitstellen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E]{1,104}$`

Erforderlich: Nein

Antwortsyntax

```
{  
  "LocationArn": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[LocationArn](#)

Der ARN des SMB-Standorts, den Sie erstellt haben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Im folgenden Beispiel wird ein Speicherort für einen SMB-Dateiserver erstellt.

```
{
  "AgentArns": [
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44b3nfs",
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-2345noo35nnee1123ovo3"
  ],
  "Domain": "AMAZON",
  "MountOptions": {
    "Version": "SMB3"
  },
  "Password": "string",
  "ServerHostname": "MyServer.amazon.com",
  "Subdirectory": "share",
  "Tags": [
    {
      "Key": "department",
      "Value": "finance"
    }
  ],
  "User": "user-1"
}
```

Beispielantwort

Eine Antwort gibt den Standort-ARN Ihres SMB-Dateiservers zurück.

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/loc-0f01451b140b2af49"
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

CreateTask

Konfiguriert eine Aufgabe, die definiert, wo und wie Ihre Daten AWS DataSync übertragen werden.

Eine Aufgabe umfasst einen Quellstandort, einen Zielort und Übertragungsoptionen (wie Bandbreitenbeschränkungen, Planung und mehr).

Important

Wenn Sie planen, Daten zu oder von einem Amazon S3 S3-Standort zu übertragen, lesen Sie zunächst, [wie sich dies auf Ihre S3-Anforderungsgebühren auswirken DataSync kann](#), sowie auf der [DataSync Preisseite](#).

Anforderungssyntax

```
{
  "CloudWatchLogGroupArn": "string",
  "DestinationLocationArn": "string",
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
      }
    }
  }
}
```

```

},
"Name": "string",
"Options": {
  "Atime": "string",
  "BytesPerSecond": number,
  "Gid": "string",
  "LogLevel": "string",
  "Mtime": "string",
  "ObjectTags": "string",
  "OverwriteMode": "string",
  "PosixPermissions": "string",
  "PreserveDeletedFiles": "string",
  "PreserveDevices": "string",
  "SecurityDescriptorCopyFlags": "string",
  "TaskQueueing": "string",
  "TransferMode": "string",
  "Uid": "string",
  "VerifyMode": "string"
},
"Schedule": {
  "ScheduleExpression": "string",
  "Status": "string"
},
"SourceLocationArn": "string",
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"TaskMode": "string",
"TaskReportConfig": {
  "Destination": {
    "S3": {
      "BucketAccessRoleArn": "string",
      "S3BucketArn": "string",
      "Subdirectory": "string"
    }
  },
  "ObjectVersionIds": "string",
  "OutputType": "string",
  "Overrides": {
    "Deleted": {
      "ReportLevel": "string"
    }
  }
}

```

```

    },
    "Skipped": {
      "ReportLevel": "string"
    },
    "Transferred": {
      "ReportLevel": "string"
    },
    "Verified": {
      "ReportLevel": "string"
    }
  },
  "ReportLevel": "string"
}

```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[CloudWatchLogGroupArn](#)

Gibt den Amazon-Ressourcennamen (ARN) einer CloudWatch Amazon-Protokollgruppe zur Überwachung Ihrer Aufgabe an.

Für Aufgaben im erweiterten Modus müssen Sie nichts angeben. DataSync sendet automatisch Protokolle an eine CloudWatch Protokollgruppe mit dem Namen `/aws/datasync`.

Weitere Informationen finden Sie unter [Überwachen von Datenübertragungen mit CloudWatch Protokollen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 562.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)?$`

Erforderlich: Nein

DestinationLocationArn

Gibt den ARN des Zielorts Ihrer Übertragung an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Excludes

Gibt Ausschlussfilter an, die die Dateien, Objekte und Ordner an Ihrem Quellspeicherort definieren, die Sie nicht übertragen DataSync möchten. Weitere Informationen und Beispiele finden Sie unter [Mithilfe von Filtern angeben, welche DataSync Übertragungen übertragen werden](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

Erforderlich: Nein

Includes

Gibt Inklusivfilter an, die die Dateien, Objekte und Ordner an Ihrem Quellspeicherort definieren, die Sie übertragen DataSync möchten. Weitere Informationen und Beispiele finden Sie unter [Mithilfe von Filtern angeben, welche DataSync Übertragungen übertragen werden](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

Erforderlich: Nein

ManifestConfig

Konfiguriert ein Manifest, bei dem es sich um eine Liste von Dateien oder Objekten handelt, die Sie übertragen DataSync möchten. Weitere Informationen und Konfigurationsbeispiele finden Sie unter [Mithilfe eines Manifests angeben, was DataSync übertragen werden soll](#).

Wenn Sie diesen Parameter verwenden, muss Ihre Anruferidentität (die Rolle, DataSync mit der Sie ihn verwenden) über die `iam:PassRole` entsprechende Berechtigung verfügen. Die [AWSDataSyncFullAccess](#) Richtlinie beinhaltet diese Erlaubnis.

Typ: [ManifestConfig](#) Objekt

Erforderlich: Nein

Name

Gibt den Namen Ihrer Aufgabe an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Erforderlich: Nein

Options

Gibt die Einstellungen Ihrer Aufgabe an, z. B. die Beibehaltung von Dateimetadaten, die Überprüfung der Datenintegrität und andere Optionen.

Typ: [Options](#) Objekt

Erforderlich: Nein

Schedule

Gibt einen Zeitplan an, zu dem Ihre Aufgabe ausgeführt werden soll. Weitere Informationen finden Sie unter [Aufgabenplanung](#).

Typ: [TaskSchedule](#) Objekt

Erforderlich: Nein

SourceLocationArn

Gibt den ARN des Quellorts Ihrer Übertragung an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Tags

Gibt die Tags an, die Sie auf Ihre Aufgabe anwenden möchten.

Stichwörter sind Schlüssel-Wert-Paare, die Ihnen helfen, Ihre DataSync Ressourcen zu verwalten, zu filtern und nach ihnen zu suchen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

TaskMode

Gibt einen der folgenden Aufgabenmodi für Ihre Datenübertragung an:

- **ENHANCED**- Übertragen Sie eine praktisch unbegrenzte Anzahl von Objekten mit höherer Leistung als im Basismodus. Aufgaben im erweiterten Modus optimieren den Datenübertragungsprozess, indem sie Daten parallel auflisten, vorbereiten, übertragen und verifizieren. Der erweiterte Modus ist derzeit für Übertragungen zwischen Amazon S3-Standorten, Übertragungen zwischen Azure Blob und Amazon S3 ohne Agenten und Übertragungen zwischen anderen Clouds und Amazon S3 ohne Agenten verfügbar.

Note

Um eine Aufgabe im erweiterten Modus zu erstellen, muss die IAM-Rolle, mit der Sie den `CreateTask` Vorgang aufrufen, über die entsprechende Berechtigung verfügen.
`iam:CreateServiceLinkedRole`

- **BASIC(Standard)** — Übertragen Sie Dateien oder Objekte zwischen dem AWS Speicher und allen anderen unterstützten DataSync Speicherorten. Für Aufgaben im Basismodus gelten [Kontingente](#) für die Anzahl der Dateien, Objekte und Verzeichnisse in einem Datensatz. Im Basismodus werden Daten sequenziell vorbereitet, übertragen und überprüft, sodass er für die meisten Workloads langsamer ist als der erweiterte Modus.

Weitere Informationen finden Sie unter [Grundlegendes zu Unterschieden im Aufgabenmodus](#).

Typ: Zeichenfolge

Zulässige Werte: BASIC | ENHANCED

Erforderlich: Nein

[TaskReportConfig](#)

Gibt an, wie Sie einen Aufgabenbericht konfigurieren möchten, der detaillierte Informationen zu Ihrer DataSync Übertragung enthält. Weitere Informationen finden Sie unter [Überwachen Ihrer DataSync Übertragungen mit Aufgabenberichten](#).

Wenn Sie diesen Parameter verwenden, muss Ihre Anruferidentität (die Rolle, DataSync mit der Sie ihn verwenden) über die `iam:PassRole` entsprechende Berechtigung verfügen. Die [AWSDataSyncFullAccess](#) Richtlinie beinhaltet diese Erlaubnis.

Typ: [TaskReportConfig](#) Objekt

Erforderlich: Nein

Antwortsyntax

```
{  
  "TaskArn": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[TaskArn](#)

Der Amazon-Ressourcenname (ARN) der Aufgabe.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung für eine Aufgabe im erweiterten Modus

Im folgenden Beispiel wird eine DataSync Aufgabe erstellt, die den erweiterten Modus verwendet.

Anders als bei der Erstellung von Aufgaben im Basismodus müssen Sie keine CloudWatch Amazon-Protokollgruppe angeben. Bei Aufgaben im erweiterten Modus werden Aufgabenprotokolle DataSync automatisch an eine Protokollgruppe mit dem Namen `gesendet/aws/datasync`. Wenn diese Protokollgruppe in Ihrer nicht vorhanden ist AWS-Region, DataSync erstellt die Protokollgruppe in Ihrem Namen, wenn Sie die Aufgabe erstellen.

```
{
  "SourceLocationArn": "arn:aws:datasync:us-east-1:111222333444:location/1111aaaa2222bbbb3",
  "DestinationLocationArn": "arn:aws:datasync:us-east-1:111222333444:location/0000zzzz1111yyyy2",
  "Name": "My Enhanced mode task",
  "TaskMode": "ENHANCED",
  "Options": {
    "TransferMode": "CHANGED",
```

```

    "VerifyMode": "ONLY_FILES_TRANSFERRED",
    "ObjectTags": "PRESERVE",
    "LogLevel": "TRANSFER"
  }
}

```

Beispielanforderung für eine Aufgabe im Basismodus

Im folgenden Beispiel wird eine DataSync Aufgabe erstellt, die den Basismodus verwendet.

```

{
  "SourceLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-1111aaaa2222bbbb3",
  "DestinationLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-0000zzzz1111yyyy2",
  "Name": "My Basic mode task",
  "TaskMode": "BASIC",
  "Options": {
    "Atime": "BEST_EFFORT",
    "Gid": "NONE",
    "Mtime": "PRESERVE",
    "PosixPermissions": "PRESERVE",
    "PreserveDevices": "NONE",
    "PreserveDeletedFiles": "PRESERVE",
    "Uid": "NONE",
    "VerifyMode": "ONLY_FILES_TRANSFERRED"
  },
  "Schedule": {
    "ScheduleExpression": "0 12 ? * SUN,WED *"
  },
  "CloudWatchLogGroupArn": "arn:aws:logs:us-east-2:111222333444:log-group:/log-group-name:*",
  "Tags": [
    {
      "Key": "Name",
      "Value": "Migration-wave-1"
    }
  ]
}

```

Beispielantwort

Die folgende Antwort enthält den ARN einer erstellten Aufgabe.

```
{  
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"  
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DeleteAgent

Entfernt eine AWS DataSync Agentenressource von Ihrer AWS-Konto.

Beachten Sie, dass durch diesen Vorgang (der nicht rückgängig gemacht werden kann) die virtuelle Maschine (VM) oder EC2 Amazon-Instanz des Agenten nicht aus Ihrer Speicherumgebung entfernt wird. Für die nächsten Schritte können Sie die VM oder Instance aus Ihrer Speicherumgebung löschen oder sie wiederverwenden, um [einen neuen Agenten zu aktivieren](#).

Anforderungssyntax

```
{  
  "AgentArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AgentArn](#)

Der Amazon-Ressourcenname (ARN) des zu löschenden Agenten. Verwenden Sie den ListAgents Vorgang, um eine Liste von Agenten für Ihr Konto und zurückzugeben AWS-Region.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DeleteLocation

Löscht eine Transferstandortressource von AWS DataSync.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Der Amazon-Ressourcenname (ARN) des Speicherorts, der gelöscht werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DeleteTask

Löscht eine Transferaufgabenressource von AWS DataSync.

Anforderungssyntax

```
{  
  "TaskArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[TaskArn](#)

Gibt den Amazon-Ressourcennamen (ARN) der Aufgabe an, die Sie löschen möchten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeAgent

Gibt Informationen über einen AWS DataSync Agenten zurück, z. B. seinen Namen, seinen Dienstendpunkttyp und seinen Status.

Anforderungssyntax

```
{  
  "AgentArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AgentArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des DataSync Agenten an, über den Sie Informationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "AgentArn": "string",  
  "CreationTime": number,  
  "EndpointType": "string",  
  "LastConnectionTime": number,  
  "Name": "string",  
  "Plattform": {
```

```

    "Version": "string"
  },
  "PrivateLinkConfig": {
    "PrivateLinkEndpoint": "string",
    "SecurityGroupArns": [ "string " ],
    "SubnetArns": [ "string " ],
    "VpcEndpointId": "string"
  },
  "Status": "string"
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AgentArn

Der ARN des Kundendienstmitarbeiters.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

Der Zeitpunkt, zu dem der Agent [aktiviert](#) wurde.

Typ: Zeitstempel

EndpointType

Der Typ des [Dienstendpunkts](#), mit dem Ihr Agent verbunden ist.

Typ: Zeichenfolge

Zulässige Werte: PUBLIC | PRIVATE_LINK | FIPS | FIPS_PRIVATE_LINK

LastConnectionTime

Das letzte Mal, dass der Agent mit dem DataSync Service kommuniziert hat.

Typ: Zeitstempel

Name

Der Name des Agenten.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/- ]+$`

Platform

Die plattformbezogenen Details zum Agenten, wie z. B. die Versionsnummer.

Typ: [Platform](#) Objekt

PrivateLinkConfig

Die Netzwerkkonfiguration, die der Agent verwendet, wenn er eine Verbindung zu einem [VPC-Dienstendpunkt](#) herstellt.

Typ: [PrivateLinkConfig](#) Objekt

Status

Der Status des Agenten.

- Wenn der Status lautet **ONLINE**, ist der Agent ordnungsgemäß konfiguriert und einsatzbereit.
- Wenn der Status lautet **OFFLINE**, hat der Agent seit fünf Minuten oder länger keinen Kontakt DataSync mehr. Dies kann verschiedene Gründe haben. Weitere Informationen finden Sie unter [Was mache ich, wenn mein Agent offline ist?](#)

Typ: Zeichenfolge

Zulässige Werte: **ONLINE** | **OFFLINE**

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Das folgende Beispiel gibt Informationen über einen in einer Anfrage angegebenen Agenten zurück.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0"
}
```

Beispielantwort

Die folgende Beispielantwort beschreibt einen Agenten, der einen öffentlichen Dienstendpunkt verwendet.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0",
  "Name": "Data center migration agent",
  "Status": "ONLINE",
  "LastConnectionTime": "2022-10-17T17:21:35.540000+00:00",
  "CreationTime": "2022-10-05T20:52:29.499000+00:00",
  "EndpointType": "PUBLIC",
  "Platform": {
    "Version": "2"
  }
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationAzureBlob

Enthält Details zur Konfiguration eines AWS DataSync Übertragungsorts für Microsoft Azure Blob Storage.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) Ihres Azure Blob Storage-Übertragungsorts an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "AccessTier": "string",  
  "AgentArns": [ "string" ],  
  "AuthenticationType": "string",  
  "BlobType": "string",  
  "CmkSecretConfig": {  
    "KmsKeyArn": "string",  
  },  
}
```

```

    "SecretArn": "string"
  },
  "CreationTime": number,
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "LocationArn": "string",
  "LocationUri": "string",
  "ManagedSecretConfig": {
    "SecretArn": "string"
  }
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[AccessTier](#)

Die Zugriffsebene, in die Ihre Objekte oder Dateien übertragen werden sollen. Dies gilt nur, wenn Sie den Standort als Übertragungsziel verwenden. Weitere Informationen finden Sie unter [Zugriffsebenen](#).

Typ: Zeichenfolge

Zulässige Werte: HOT | COOL | ARCHIVE

[AgentArns](#)

Die ARNs DataSync Agents, die eine Verbindung mit Ihrem Azure Blob Storage-Container herstellen können.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Die Authentifizierungsmethode, die für den Zugriff auf Ihren Azure Blob Storage DataSync verwendet wird. DataSync kann mithilfe einer Shared Access Signature (SAS) auf den Blob-Speicher zugreifen.

Typ: Zeichenfolge

Zulässige Werte: SAS | NONE

BlobType

Der Blobtyp, den Ihre Objekte oder Dateien haben sollen, wenn sie in Azure Blob Storage übertragen werden. Unterstützt derzeit DataSync nur das Verschieben von Daten in Azure Blob Storage als Blockblobs. Weitere Informationen zu Blobtypen finden Sie in der [Azure Blob Storage](#)-Dokumentation.

Typ: Zeichenfolge

Zulässige Werte: BLOCK

CmkSecretConfig

Beschreibt die Konfigurationsinformationen für ein vom Kunden DataSync verwaltetes Geheimnis, z. B. ein Authentifizierungstoken, das für den Zugriff auf einen bestimmten Speicherort DataSync verwendet wird, wobei ein vom Kunden verwalteter Schlüssel verwendet wird. AWS KMS key

Typ: [CmkSecretConfig](#) Objekt

CreationTime

Der Zeitpunkt, zu dem Ihr Azure Blob Storage-Übertragungsort erstellt wurde.

Typ: Zeitstempel

CustomSecretConfig

Beschreibt die Konfigurationsinformationen für ein vom Kunden verwaltetes Geheimnis, z. B. ein Authentifizierungstoken, das für den Zugriff auf einen bestimmten Speicherort DataSync verwendet wird, wobei ein vom Kunden verwalteter Schlüssel verwendet wird. AWS KMS key

Typ: [CustomSecretConfig](#) Objekt

LocationArn

Der ARN Ihres Azure Blob Storage-Übertragungsorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

Die URL des Azure Blob Storage-Containers, der an Ihrer Übertragung beteiligt ist.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[ManagedSecretConfig](#)

Beschreibt die Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis, z. B. ein Authentifizierungstoken, das für den Zugriff auf einen bestimmten Speicherort DataSync verwendet wird. DataSync verwendet den standardmäßigen AWS verwalteten KMS-Schlüssel, um dieses Geheimnis zu verschlüsseln. AWS Secrets Manager

Typ: [ManagedSecretConfig](#) Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im Dienst ein Fehler auftritt. AWS DataSync

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationEfs

Enthält Details darüber, wie ein AWS DataSync Übertragungsort für ein Amazon EFS-Dateisystem konfiguriert ist.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[LocationArn](#)

Der Amazon-Ressourcenname (ARN) des Amazon EFS-Dateisystemspeicherorts, über den Sie Informationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "AccessPointArn": "string",  
  "CreationTime": number,  
  "Ec2Config": {  
    "SecurityGroupArns": [ "string" ],  
    "SubnetArn": "string"  
  },  
}
```

```
"FileSystemAccessRoleArn": "string",  
"InTransitEncryption": "string",  
"LocationArn": "string",  
"LocationUri": "string"  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[AccessPointArn](#)

Der ARN des Access Points, der für den Zugriff auf das Amazon EFS-Dateisystem DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugreifen auf eingeschränkte Dateisysteme](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

[CreationTime](#)

Der Zeitpunkt, zu dem der Standort erstellt wurde.

Typ: Zeitstempel

[Ec2Config](#)

Das Subnetz und die Sicherheitsgruppen, die für die Verbindung zu einem der [Mount-Ziele](#) Ihres Amazon EFS-Dateisystems AWS DataSync verwendet werden.

Typ: [Ec2Config](#) Objekt

[FileSystemAccessRoleArn](#)

Die AWS Identity and Access Management (IAM) -Rolle, die DataSync den Zugriff auf Ihr Amazon EFS-Dateisystem ermöglicht.

Weitere Informationen finden Sie unter [Erstellen einer DataSync IAM-Rolle für den Dateisystemzugriff](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

[InTransitEncryption](#)

Gibt an, ob bei der Übertragung von Daten zum oder vom Amazon EFS-Dateisystem die Transport Layer Security (TLS) -Verschlüsselung DataSync verwendet wird.

Typ: Zeichenfolge

Zulässige Werte: NONE | TLS1_2

[LocationArn](#)

Der ARN des Speicherorts des Amazon EFS-Dateisystems.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

Die URL des Speicherorts des Amazon EFS-Dateisystems.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Das folgende Beispiel zeigt, wie Sie Informationen über einen bestimmten Speicherort im Amazon EFS-Dateisystem abrufen können.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-12abcdef012345678"
}
```

Beispielantwort

Das folgende Beispiel gibt Standortdetails zu einem Amazon EFS-Dateisystem zurück.

```
{
  "CreationTime": 1653319021.353,
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/subnet-1234567890abcdef1",
    "SecurityGroupArns": [
      "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
    ]
  },
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-abcdef01234567890",
  "LocationUri": "efs://us-east-2.fs-021345abcdef6789/"
}
```

Beispielantwort: Beschreibung eines Speicherorts für ein eingeschränktes Amazon EFS-Dateisystem

Das folgende Beispiel gibt Standortdetails zu einem Amazon EFS-Dateisystem mit eingeschränktem Zugriff zurück `AccessPointArn`, einschließlich der `InTransitEncryption` Elemente `FileSystemAccessRoleArn`, und.

```
{
  "CreationTime": 1653319021.353,
  "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:access-point/
fsap-1234567890abcdef0",
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/
subnet-1234567890abcdef1",
    "SecurityGroupArns": [
      "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
    ]
  },
  "FileSystemAccessRoleArn": "arn:aws:iam::111222333444:role/
AwsDataSyncFullAccessNew",
  "InTransitEncryption": "TLS1_2",
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-
abcdef01234567890",
  "LocationUri": "efs://us-east-2.fs-021345abcdef6789/",
  "Subdirectory": "/mount/path",
  "Tags": [{
    "Key": "Name",
    "Value": "ElasticFileSystem-1"
  }]
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationFsxLustre

Enthält Einzelheiten zur Konfiguration eines AWS DataSync Übertragungsorts für ein Amazon FSx for Lustre-Dateisystem.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Der Amazon-Ressourcenname (ARN) des zu FSx beschreibenden for Lustre-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "CreationTime": number,  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "SecurityGroupArns": [ "string" ]  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Der Zeitpunkt, zu dem der Standort FSx für Lustre erstellt wurde.

Typ: Zeitstempel

LocationArn

Der Amazon-Ressourcenname (ARN) des beschriebenen FSx For Lustre-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

Der URI des FSx for Lustre-Standorts, der beschrieben wurde.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

Die Amazon-Ressourcenamen (ARNs) der Sicherheitsgruppen, die für das FSx for Lustre-Dateisystem konfiguriert sind.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationFsxOntap

Enthält Einzelheiten zur Konfiguration eines AWS DataSync Übertragungsorts für ein Amazon FSx for NetApp ONTAP-Dateisystem.

Note

Wenn Ihr Standort SMB verwendet, gibt der DescribeLocationFsxOntap Vorgang nicht wirklich a zurück. Password

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des Speicherorts FSx für das ONTAP-Dateisystem an, über den Sie Informationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{
```



```

"CreationTime": number,
"FsxFilesystemArn": "string",
"LocationArn": "string",
"LocationUri": "string",
"Protocol": {
  "NFS": {
    "MountOptions": {
      "Version": "string"
    }
  },
  "SMB": {
    "Domain": "string",
    "MountOptions": {
      "Version": "string"
    },
    "Password": "string",
    "User": "string"
  }
},
"SecurityGroupArns": [ "string" ],
"StorageVirtualMachineArn": "string"
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Die Uhrzeit, zu der der Standort erstellt wurde.

Typ: Zeitstempel

FsxFilesystemArn

Der ARN des FSx for ONTAP-Dateisystems.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

LocationArn

Der ARN des Speicherorts FSx für das ONTAP-Dateisystem.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

Der Uniform Resource Identifier (URI) des Speicherorts FSx für das ONTAP-Dateisystem.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

Gibt das Datenübertragungsprotokoll an, das für den Zugriff auf Ihr FSx Amazon-Dateisystem AWS DataSync verwendet wird.

Typ: [FsxProtocol](#) Objekt

SecurityGroupArns

Die Sicherheitsgruppen, die FSx für den Zugriff auf Ihr ONTAP-Dateisystem DataSync verwendet werden.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

StorageVirtualMachineArn

Der ARN der virtuellen Speichermaschine (SVM) auf Ihrem FSx ONTAP-Dateisystem, zu dem Sie Daten kopieren oder von der Sie Daten kopieren.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 162.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]+:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)

- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationFsxOpenZfs

Enthält Einzelheiten zur Konfiguration eines AWS DataSync Übertragungsorts für ein Amazon FSx for OpenZFS-Dateisystem.

Note

Antwortelemente, die sich auf beziehen, werden von dem DescribeLocationFsxOpenZfs Vorgang SMB nicht unterstützt.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Der Amazon-Ressourcenname (ARN) des zu FSx beschreibenden OpenZFS-Speicherorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{
```

```

"CreationTime": number,
"LocationArn": "string",
"LocationUri": "string",
"Protocol": {
  "NFS": {
    "MountOptions": {
      "Version": "string"
    }
  },
  "SMB": {
    "Domain": "string",
    "MountOptions": {
      "Version": "string"
    },
    "Password": "string",
    "User": "string"
  }
},
"SecurityGroupArns": [ "string" ]
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Der Zeitpunkt, zu dem der Speicherort FSx für OpenZFS erstellt wurde.

Typ: Zeitstempel

LocationArn

Der ARN des FSx für OpenZFS beschriebenen Speicherorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

Der Uniform Resource Identifier (URI) des beschriebenen Standorts FSx für OpenZFS.

Beispiel: `fsxz://us-west-2.fs-1234567890abcdef02/fsx/folderA/folder`

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[Protocol](#)

Der Protokolltyp, der für den Zugriff auf Ihr Dateisystem AWS DataSync verwendet wird.

Typ: [FsxProtocol](#) Objekt

[SecurityGroupArns](#)

Die ARNs Sicherheitsgruppen, die FSx für das OpenZFS-Dateisystem konfiguriert sind.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im Dienst ein Fehler auftritt. AWS DataSync

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationFsxWindows

Enthält Einzelheiten darüber, wie ein AWS DataSync Übertragungsort für ein Amazon FSx for Windows File Server-Dateisystem konfiguriert ist.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[LocationArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des Speicherorts FSx für den Windows-Dateiserver an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "CreationTime": number,  
  "Domain": "string",  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "SecurityGroupArns": [ "string" ],  
  "User": "string"  
}
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CreationTime

Der Zeitpunkt, zu dem der Speicherort FSx für den Windows-Dateiserver erstellt wurde.

Typ: Zeitstempel

Domain

Der Name der Microsoft Active Directory-Domäne, zu der das Dateisystem FSx für Windows File Server gehört.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}$`

LocationArn

Der ARN des Speicherorts FSx für den Windows-Dateiserver.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

Der Uniform Resource Identifier (URI) des Speicherorts FSx für den Windows-Dateiserver.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\\-]+$`

SecurityGroupArns

Die ARNs EC2 Amazon-Sicherheitsgruppen, die den Zugriff auf das bevorzugte Subnetz Ihres Dateisystems ermöglichen.

Informationen zur Konfiguration von Sicherheitsgruppen für den Dateisystemzugriff finden Sie im [Amazon FSx for Windows File Server-Benutzerhandbuch](#).

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

User

Der Benutzer mit den Berechtigungen zum Mounten und Zugreifen auf das Dateisystem FSx für Windows File Server.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\x22\x5B\x5D/\\";|, +*?\x3C\x3E]{1,104}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationHdfs

Enthält Einzelheiten zur Konfiguration eines AWS DataSync Übertragungsorts für ein Hadoop Distributed File System (HDFS).

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des HDFS-Speicherorts an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "AgentArns": [ "string" ],  
  "AuthenticationType": "string",  
  "BlockSize": number,  
  "CreationTime": number,  
  "KerberosPrincipal": "string",  
  "KmsKeyProviderUri": "string",  
  "LocationArn": "string",
```

```

"LocationUri": "string",
"NameNodes": [
  {
    "Hostname": "string",
    "Port": number
  }
],
"QopConfiguration": {
  "DataTransferProtection": "string",
  "RpcProtection": "string"
},
"ReplicationFactor": number,
"SimpleUser": "string"
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AgentArns

Der ARNs der DataSync Agenten, die eine Verbindung zu Ihrem HDFS-Cluster herstellen können.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Elementen.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Die Art der Authentifizierung, die verwendet wird, um die Identität des Benutzers zu ermitteln.

Typ: Zeichenfolge

Zulässige Werte: SIMPLE | KERBEROS

BlockSize

Die Größe der Datenblöcke, die in den HDFS-Cluster geschrieben werden sollen.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert von 1048576. Der Höchstwert ist 1073741824.

CreationTime

Der Zeitpunkt, zu dem der HDFS-Speicherort erstellt wurde.

Typ: Zeitstempel

KerberosPrincipal

Das Kerberos-Prinzipal mit Zugriff auf die Dateien und Ordner im HDFS-Cluster. Dieser Parameter wird verwendet, wenn der definiert `AuthenticationType` ist als `KERBEROS`.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^\.+`

KmsKeyProviderUri

Die URI des Key Management Servers (KMS) des HDFS-Clusters.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Pattern: `^kms:\//http[s]?@(([a-zA-Z0-9\-\_]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-\_]*[A-Za-z0-9])(;((([a-zA-Z0-9\-\_]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-\_]*[A-Za-z0-9]))*:[0-9]{1,5}\//kms$`

LocationArn

Der ARN des HDFS-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\_0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

Der URI des HDFS-Speicherorts.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

NameNodes

Der NameNode , der den HDFS-Namespace verwaltet.

Typ: Array von [HdfsNameNode](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element.

QopConfiguration

Die QOP-Konfiguration (Quality of Protection), die die auf dem HDFS-Cluster konfigurierten Einstellungen für den Remote Procedure Call (RPC) und den Schutz der Datenübertragung festlegt.

Typ: [QopConfiguration](#) Objekt

ReplicationFactor

Die Nummer DataNodes , auf die die Daten repliziert werden sollen, wenn in den HDFS-Cluster geschrieben wird.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Der Maximalwert ist 512.

SimpleUser

Der Benutzername zur Identifizierung des Clients auf dem Host-Betriebssystem. Dieser Parameter wird verwendet, wenn der definiert `AuthenticationType` ist als `SIMPLE`.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[_ .A-Za-z0-9][-_ .A-Za-z0-9]*$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationNfs

Enthält Einzelheiten zur Konfiguration eines AWS DataSync Übertragungsorts für einen NFS-Dateiserver (Network File System).

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des NFS-Speicherorts an, über den Sie Informationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "CreationTime": number,  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "MountOptions": {  
    "Version": "string"  
  }  
}
```

```
  },  
  "OnPremConfig": {  
    "AgentArns": [ "string" ]  
  }  
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[CreationTime](#)

Die Uhrzeit, zu der der NFS-Standort erstellt wurde.

Typ: Zeitstempel

[LocationArn](#)

Der ARN des NFS-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

Die URI des NFS-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[MountOptions](#)

Die Mount-Optionen, die zum Mounten Ihres NFS-Dateiservers DataSync verwendet werden.

Typ: [NfsMountOptions](#) Objekt

[OnPremConfig](#)

Die AWS DataSync Agenten, die eine Verbindung zu Ihrem NFS-Dateiserver (Network File System) herstellen können.

Typ: [OnPremConfig](#) Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispiel

Das folgende Beispiel gibt Informationen über den in der Beispielanforderung angegebenen NFS-Speicherort zurück.

Beispielanforderung

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

Beispiel

Dieses Beispiel veranschaulicht eine Verwendung von `DescribeLocationNfs`

Beispielantwort

```
{
  "CreationTime": 1532660733.39,
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-07db7abfc326c50aa",
  "LocationUri": "hostname.amazon.com",
  "OnPremConfig": {
    "AgentArns": [ "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44b3nfs" ]
  }
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationObjectStorage

Enthält Details zur Konfiguration eines AWS DataSync Übertragungsorts für ein Objektspeichersystem.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des Objektspeichersystems an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "AccessKey": "string",  
  "AgentArns": [ "string" ],  
  "CmkSecretConfig": {  
    "KmsKeyArn": "string",  
    "SecretArn": "string"  
  },  
  "CreationTime": number,  
}
```

```

"CustomSecretConfig": {
  "SecretAccessRoleArn": "string",
  "SecretArn": "string"
},
"LocationArn": "string",
"LocationUri": "string",
"ManagedSecretConfig": {
  "SecretArn": "string"
},
"ServerCertificate": blob,
"ServerPort": number,
"ServerProtocol": "string"
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AccessKey

Der Zugriffsschlüssel (z. B. ein Benutzername), der für die Authentifizierung beim Objektspeichersystem erforderlich ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Höchstlänge = 200 Zeichen.

Pattern: ^.*\$

AgentArns

Der ARNs der DataSync Agenten, die eine Verbindung zu Ihrem Objektspeichersystem herstellen können.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: ^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}\$

[CmkSecretConfig](#)

Beschreibt die Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis, z. B. ein Authentifizierungstoken oder einen Satz von Anmeldeinformationen, das für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet wird, und für einen vom Kunden AWS KMS key verwalteten Schlüssel.

Typ: [CmkSecretConfig](#) Objekt

[CreationTime](#)

Der Zeitpunkt, zu dem der Standort erstellt wurde.

Typ: Zeitstempel

[CustomSecretConfig](#)

Beschreibt die Konfigurationsinformationen für ein vom Kunden verwaltetes Geheimnis, wie z. B. ein Authentifizierungstoken oder einen Satz von Anmeldeinformationen, das für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet wird, und für ein vom Kunden AWS KMS key verwaltetes Geheimnis.

Typ: [CustomSecretConfig](#) Objekt

[LocationArn](#)

Der ARN des Objekt-Storage-Systemstandorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

Die URI des Speicherorts des Objektspeichersystems.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[ManagedSecretConfig](#)

Beschreibt die Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis, wie z. B. ein Authentifizierungstoken oder eine Reihe von Anmeldeinformationen, die für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet werden. DataSync verwendet den standardmäßigen AWS verwalteten KMS-Schlüssel, um dieses Geheimnis zu verschlüsseln. AWS Secrets Manager

Typ: [ManagedSecretConfig](#) Objekt

[ServerCertificate](#)

Die Zertifikatskette für DataSync die Authentifizierung bei Ihrem Objektspeichersystem, wenn das System eine private oder selbstsignierte Zertifizierungsstelle (CA) verwendet.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 32768.

[ServerPort](#)

Der Port, über den Ihr Object Storage-Server eingehenden Netzwerkverkehr akzeptiert (z. B. Port 443).

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Der Maximalwert ist 65536.

[ServerProtocol](#)

Das Protokoll, das Ihr Objektspeichersystem für die Kommunikation verwendet.

Typ: Zeichenfolge

Zulässige Werte: HTTPS | HTTP

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationS3

Enthält Einzelheiten zur Konfiguration eines AWS DataSync Übertragungsorts für einen S3-Bucket.

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des Amazon S3-Standorts an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "AgentArns": [ "string" ],  
  "CreationTime": number,  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "S3Config": {  
    "BucketAccessRoleArn": "string"  
  },  
  "S3StorageClass": "string"  
}
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AgentArns

Die ARNs DataSync Agenten, die auf Ihrem Outpost eingesetzt wurden, wenn Sie mit Amazon S3 auf Outposts arbeiten.

Weitere Informationen finden Sie unter [Bereitstellen Ihres DataSync Agenten auf](#) AWS Outposts

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

Der Zeitpunkt, zu dem der Amazon S3 S3-Standort erstellt wurde.

Typ: Zeitstempel

LocationArn

Der ARN des Amazon S3 S3-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

Die URL des Amazon S3 S3-Standorts, der beschrieben wurde.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

S3Config

Gibt den Amazon-Ressourcennamen (ARN) der AWS Identity and Access Management (IAM) - Rolle an, die für den Zugriff auf Ihren S3-Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [DataSync Zugriff auf S3-Buckets bereitstellen](#).

Typ: [S3Config](#) Objekt

S3StorageClass

Wenn Amazon S3 ein Zielort ist, ist dies die Speicherklasse, die Sie für Ihre Objekte ausgewählt haben.

Einige Speicherklassen weisen Verhaltensweisen auf, die sich auf Ihre Amazon S3 S3-Speicherkosten auswirken können. Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#).

Typ: Zeichenfolge

Zulässige Werte: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispiel

Das folgende Beispiel gibt Informationen über den Amazon S3 S3-Standort zurück, der in der Beispielanforderung angegeben wurde.

Beispielanforderung

```
{
  "LocationArn": "arn:aws:datsync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

Beispiel

Dieses Beispiel veranschaulicht eine Verwendung von DescribeLocation S3.

Beispielantwort

```
{
  "CreationTime": 1532660733.39,
  "LocationArn": "arn:aws:datsync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3",
  "LocationUri": "s3://amzn-s3-demo-bucket",
  "S3Config": {
    "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/amzn-s3-demo-bucket-
access-role",
  }
  "S3StorageClass": "STANDARD"
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeLocationSmb

Enthält Einzelheiten zur Konfiguration eines AWS DataSync Übertragungsorts für einen SMB-Dateiserver (Server Message Block).

Anforderungssyntax

```
{  
  "LocationArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[LocationArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des SMB-Standorts an, über den Sie Informationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "AgentArns": [ "string" ],  
  "AuthenticationType": "string",  
  "CmkSecretConfig": {  
    "KmsKeyArn": "string",  
    "SecretArn": "string"  
  }  
}
```



```

},
"CreationTime": number,
"CustomSecretConfig": {
  "SecretAccessRoleArn": "string",
  "SecretArn": "string"
},
"DnsIpAddresses": [ "string" ],
"Domain": "string",
"KerberosPrincipal": "string",
"LocationArn": "string",
"LocationUri": "string",
"ManagedSecretConfig": {
  "SecretArn": "string"
},
"MountOptions": {
  "Version": "string"
},
"User": "string"
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AgentArns

Die DataSync Agenten, ARNs die eine Verbindung zu Ihrem SMB-Dateiserver herstellen können.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Das Authentifizierungsprotokoll, das für die Verbindung mit Ihrem SMB-Dateiserver DataSync verwendet wird.

Typ: Zeichenfolge

Zulässige Werte: NTLM | KERBEROS

CmkSecretConfig

Beschreibt die Konfigurationsinformationen für ein DataSync vom Kunden verwaltetes Geheimnis, wie z. B. ein Password oder KerberosKeytab, das für den Zugriff auf einen bestimmten Speicherort DataSync verwendet wird. AWS KMS key

Typ: [CmkSecretConfig](#) Objekt

CreationTime

Der Zeitpunkt, zu dem der SMB-Standort erstellt wurde.

Typ: Zeitstempel

CustomSecretConfig

Beschreibt die Konfigurationsinformationen für ein vom Kunden verwaltetes Geheimnis, wie z. B. ein Password oder, KerberosKeytab das für den Zugriff auf einen bestimmten Speicherort DataSync verwendet wird, mit einem vom Kunden verwalteten Geheimnis. AWS KMS key

Typ: [CustomSecretConfig](#) Objekt

DnsIpAddresses

Die IPv6 Adressen IPv4 oder für die DNS-Server, zu denen Ihr SMB-Dateiserver gehört. Dieses Element gilt nur, wenn AuthenticationType es auf KERBEROS gesetzt ist.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Maximale Anzahl von 2 Elementen.

Längenbeschränkungen: Minimale Länge beträgt 7 Zeichen. Die maximale Länge beträgt 39.

Pattern: `\A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\. (25[0-5]|2[0-4]\d|[0-1]?\d?\d))){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}: [0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(: [0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(: [0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(: [0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(: [0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((: [0-9a-fA-F]{1,4}){1,6}))\z`

Domain

Der Name der Windows-Domäne, zu der der SMB-Dateiserver gehört. Dieses Element gilt nur, wenn `AuthenticationType` es auf NTLM gesetzt ist.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}$`

KerberosPrincipal

Der Kerberos-Prinzipal, der berechtigt ist, auf die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver zuzugreifen.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^\\.+`

LocationArn

Der ARN des SMB-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

Die URI des SMB-Standorts.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:\\-]+$`

[ManagedSecretConfig](#)

Beschreibt die Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis, wie z. B. ein Password oder, KerberosKeytab das für den Zugriff auf einen bestimmten Speicherort DataSync verwendet wird. DataSync verwendet den standardmäßigen AWS verwalteten KMS-Schlüssel, um dieses Geheimnis zu verschlüsseln. AWS Secrets Manager

Typ: [ManagedSecretConfig](#) Objekt

[MountOptions](#)

Die SMB-Protokollversion, die für den Zugriff auf Ihren SMB-Dateiserver DataSync verwendet wird.

Typ: [SmbMountOptions](#) Objekt

[User](#)

Der Benutzer, der die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver bereitstellen und darauf zugreifen kann. Dieses Element gilt nur, wenn AuthenticationType es auf NTLM gesetzt ist.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\x22\x5B\x5D/\\";|=, +*?\x3C\x3E]{1,104}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispiel

Dieses Beispiel veranschaulicht eine Verwendung von `DescribeLocationSmb`

Beispielanforderung

```
{
  "arn:aws:datasync:us-east-1:111222333444:location/loc-0f01451b140b2af49"
}
```

Beispiel

Dieses Beispiel veranschaulicht eine Verwendung von `DescribeLocationSmb`.

Beispielantwort

```
{
  "AgentArns": [
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-0bc3b3dc9bbc15145",
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-04b3fe3d261a18c8f"
  ],
  "CreationTime": "1532660733.39",
  "Domain": "AMAZON",
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/loc-0f01451b140b2af49",
  "LocationUri": "smb://hostname.amazon.com/share",
  "MountOptions": {
    "Version": "SMB3"
  },
  "User": "user-1"
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

DescribeTask

Stellt Informationen zu einer Aufgabe bereit, die definiert, wo und wie Ihre Daten AWS DataSync übertragen werden.

Anforderungssyntax

```
{  
  "TaskArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

TaskArn

Gibt den Amazon-Ressourcennamen (ARN) der Übertragungsaufgabe an, über die Sie Informationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{  
  "CloudWatchLogGroupArn": "string",  
  "CreationTime": number,  
  "CurrentTaskExecutionArn": "string",  
  "DestinationLocationArn": "string",  
  "DestinationNetworkInterfaceArns": [ "string" ],  
  "ErrorCode": "string",  
  "ErrorDetail": "string",  
}
```

```

    "Excludes": [
      {
        "FilterType": "string",
        "Value": "string"
      }
    ],
    "Includes": [
      {
        "FilterType": "string",
        "Value": "string"
      }
    ],
    "ManifestConfig": {
      "Action": "string",
      "Format": "string",
      "Source": {
        "S3": {
          "BucketAccessRoleArn": "string",
          "ManifestObjectPath": "string",
          "ManifestObjectVersionId": "string",
          "S3BucketArn": "string"
        }
      }
    },
    "Name": "string",
    "Options": {
      "Atime": "string",
      "BytesPerSecond": number,
      "Gid": "string",
      "LogLevel": "string",
      "Mtime": "string",
      "ObjectTags": "string",
      "OverwriteMode": "string",
      "PosixPermissions": "string",
      "PreserveDeletedFiles": "string",
      "PreserveDevices": "string",
      "SecurityDescriptorCopyFlags": "string",
      "TaskQueueing": "string",
      "TransferMode": "string",
      "Uid": "string",
      "VerifyMode": "string"
    },
    "Schedule": {
      "ScheduleExpression": "string",

```



```

    "Status": "string"
  },
  "ScheduleDetails": {
    "DisabledBy": "string",
    "DisabledReason": "string",
    "StatusUpdateTime": number
  },
  "SourceLocationArn": "string",
  "SourceNetworkInterfaceArns": [ "string " ],
  "Status": "string",
  "TaskArn": "string",
  "TaskMode": "string",
  "TaskReportConfig": {
    "Destination": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "S3BucketArn": "string",
        "Subdirectory": "string"
      }
    },
    "ObjectVersionIds": "string",
    "OutputType": "string",
    "Overrides": {
      "Deleted": {
        "ReportLevel": "string"
      },
      "Skipped": {
        "ReportLevel": "string"
      },
      "Transferred": {
        "ReportLevel": "string"
      },
      "Verified": {
        "ReportLevel": "string"
      }
    }
  },
  "ReportLevel": "string"
}
}

```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

CloudWatchLogGroupArn

Der Amazon-Ressourcenname (ARN) einer CloudWatch Amazon-Protokollgruppe zur Überwachung Ihrer Aufgabe.

Weitere Informationen finden Sie unter [Überwachen von Datenübertragungen mit CloudWatch Protokollen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 562.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)*$`

CreationTime

Der Zeitpunkt, zu dem die Aufgabe erstellt wurde.

Typ: Zeitstempel

CurrentTaskExecutionArn

Der ARN der letzten Aufgabenausführung.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

DestinationLocationArn

Der ARN des Zielorts Ihrer Übertragung.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

DestinationNetworkInterfaceArns

Die ARNs [Netzwerkschnittstellen](#), die für Ihren Zielort DataSync erstellt wurden.

Typ: Zeichenfolgen-Array

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-\0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

ErrorCode

Wenn bei Ihrer Aufgabe ein Problem auftritt, können Sie den Fehlercode verwenden, um das Problem zu beheben. Weitere Informationen finden Sie unter [Problembehandlung bei DataSync Übertragungen](#).

Typ: Zeichenfolge

ErrorDetail

Wenn bei Ihrer Aufgabe ein Problem auftritt, können Sie die Fehlerdetails verwenden, um das Problem zu beheben. Weitere Informationen finden Sie unter [Problembehandlung bei DataSync Übertragungen](#).

Typ: Zeichenfolge

Excludes

Die Ausschlussfilter, die die Dateien, Objekte und Ordner an Ihrem Quellspeicherort definieren, die Sie nicht übertragen DataSync möchten. Weitere Informationen und Beispiele finden Sie unter [Mithilfe von Filtern angeben, welche DataSync Übertragungen übertragen werden](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

Includes

Dazu gehören Filter, die die Dateien, Objekte und Ordner an Ihrem Quellspeicherort definieren, die Sie übertragen DataSync möchten. Weitere Informationen und Beispiele finden Sie unter [Mithilfe von Filtern angeben, welche DataSync Übertragungen übertragen werden](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

ManifestConfig

Die Konfiguration des Manifests, das die Dateien oder Objekte auflistet, die Sie übertragen DataSync möchten. Weitere Informationen finden Sie unter [Mithilfe eines Manifests angeben, welche DataSync Übertragungen übertragen](#) werden.

Typ: [ManifestConfig](#) Objekt

Name

Der Name Ihrer Aufgabe.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/- ]+$`

Options

Die Einstellungen der Aufgabe. Beispielsweise, welche Dateimetadaten erhalten bleiben, wie die Datenintegrität am Ende der Übertragung überprüft wird, Bandbreitenbeschränkungen und andere Optionen.

Typ: [Options](#) Objekt

Schedule

Der Zeitplan, zu dem Ihre Aufgabe ausgeführt werden soll. Weitere Informationen finden Sie unter [Aufgabenplanung](#).

Typ: [TaskSchedule](#) Objekt

ScheduleDetails

Die Details zu Ihrem [Task-Zeitplan](#).

Typ: [TaskScheduleDetails](#) Objekt

SourceLocationArn

Der ARN des Quellorts Ihrer Übertragung.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

SourceNetworkInterfaceArns

Die ARNs [Netzwerkschnittstellen](#), die für Ihren Quellstandort DataSync erstellt wurden.

Typ: Zeichenfolgen-Array

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-\0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

Status

Der Status Ihrer Aufgabe. Informationen zur Bedeutung der einzelnen Status finden Sie unter [Aufgabenstatus](#).

Typ: Zeichenfolge

Zulässige Werte: AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE

TaskArn

Der ARN Ihrer Aufgabe.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

TaskMode

Der Aufgabenmodus, den Sie verwenden. Weitere Informationen finden Sie unter [Auswählen eines Aufgabenmodus für Ihre Datenübertragung](#).

Typ: Zeichenfolge

Zulässige Werte: BASIC | ENHANCED

[TaskReportConfig](#)

Die Konfiguration Ihres Aufgabenberichts, der detaillierte Informationen zu Ihrer DataSync Übertragung enthält. Weitere Informationen finden Sie unter [Überwachen Ihrer DataSync Übertragungen mit Aufgabenberichten](#).

Typ: [TaskReportConfig](#) Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Das folgende Beispiel gibt den ARN einer DataSync Aufgabe an, über die Informationen abgerufen werden sollen.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Beispielantwort

Das folgende Beispiel zeigt eine DescribeTask Antwort.

```
{
```

```

"TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026",
"Name": "MyTask",
"TaskMode": "BASIC",
"Status": "RUNNING",
"SourceLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-1111aaaa2222bbbb3",
"DestinationLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-0000zzzz1111yyyy2",
"CurrentTaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f",
"CreationTime": 1532660733.39,
"Options": {
  "Atime": "BEST_EFFORT",
  "BytesPerSecond": 1000,
  "Gid": "NONE",
  "Mtime": "PRESERVE",
  "PosixPermissions": "PRESERVE",
  "PreserveDevices": "NONE",
  "PreserveDeletedFiles": "PRESERVE",
  "Uid": "NONE",
  "VerifyMode": "POINT_IN_TIME_CONSISTENT"
},
"CloudWatchLogGroupArn": "arn:aws:logs:us-east-2:111222333444:log-group:/log-group-
name:*"
}

```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)

- [AWS SDK for Ruby V3](#)

DescribeTaskExecution

Stellt Informationen über die Ausführung Ihrer AWS DataSync Aufgabe bereit. Sie können diesen Vorgang verwenden, um den Fortschritt einer laufenden Datenübertragung zu überwachen oder die Ergebnisse der Übertragung zu überprüfen.

Note

Einige DescribeTaskExecution Antwortelemente sind nur für einen bestimmten Aufgabenmodus relevant. Weitere Informationen finden Sie unter [Grundlegendes zu Unterschieden im Aufgabenmodus](#) und [Grundlegendes zu Leistungsindikatoren bei der Datenübertragung](#).

Anforderungssyntax

```
{  
  "TaskExecutionArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[TaskExecutionArn](#)

Gibt den Amazon-Ressourcennamen (ARN) der Aufgabenausführung an, über die Sie Informationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Erforderlich: Ja

Antwortsyntax

```
{
  "BytesCompressed": number,
  "BytesTransferred": number,
  "BytesWritten": number,
  "EndTime": number,
  "EstimatedBytesToTransfer": number,
  "EstimatedFilesToDelete": number,
  "EstimatedFilesToTransfer": number,
  "EstimatedFoldersToDelete": number,
  "EstimatedFoldersToTransfer": number,
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "FilesDeleted": number,
  "FilesFailed": {
    "Delete": number,
    "Prepare": number,
    "Transfer": number,
    "Verify": number
  },
  "FilesListed": {
    "AtDestinationForDelete": number,
    "AtSource": number
  },
  "FilesPrepared": number,
  "FilesSkipped": number,
  "FilesTransferred": number,
  "FilesVerified": number,
  "FoldersDeleted": number,
  "FoldersFailed": {
    "Delete": number,
    "List": number,
    "Prepare": number,
    "Transfer": number,
    "Verify": number
  },
  "FoldersListed": {
    "AtDestinationForDelete": number,
```

```

    "AtSource": number
  },
  "FoldersPrepared": number,
  "FoldersSkipped": number,
  "FoldersTransferred": number,
  "FoldersVerified": number,
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "LaunchTime": number,
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
      }
    }
  },
  "Options": {
    "Atime": "string",
    "BytesPerSecond": number,
    "Gid": "string",
    "LogLevel": "string",
    "Mtime": "string",
    "ObjectTags": "string",
    "OverwriteMode": "string",
    "PosixPermissions": "string",
    "PreserveDeletedFiles": "string",
    "PreserveDevices": "string",
    "SecurityDescriptorCopyFlags": "string",
    "TaskQueueing": "string",
    "TransferMode": "string",
    "Uid": "string",
    "VerifyMode": "string"
  },
  "ReportResult": {
    "ErrorCode": "string",

```

```

    "ErrorDetail": "string",
    "Status": "string"
  },
  "Result": {
    "ErrorCode": "string",
    "ErrorDetail": "string",
    "PrepareDuration": number,
    "PrepareStatus": "string",
    "TotalDuration": number,
    "TransferDuration": number,
    "TransferStatus": "string",
    "VerifyDuration": number,
    "VerifyStatus": "string"
  },
  "StartTime": number,
  "Status": "string",
  "TaskExecutionArn": "string",
  "TaskMode": "string",
  "TaskReportConfig": {
    "Destination": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "S3BucketArn": "string",
        "Subdirectory": "string"
      }
    },
    "ObjectVersionIds": "string",
    "OutputType": "string",
    "Overrides": {
      "Deleted": {
        "ReportLevel": "string"
      },
      "Skipped": {
        "ReportLevel": "string"
      },
      "Transferred": {
        "ReportLevel": "string"
      },
      "Verified": {
        "ReportLevel": "string"
      }
    }
  },
  "ReportLevel": "string"
}

```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[BytesCompressed](#)

Die Anzahl der physischen Byte, die nach der Komprimierung über das Netzwerk DataSync übertragen werden (sofern eine Komprimierung möglich ist). Diese Zahl ist in der Regel geringer als, [BytesTransferred](#) sofern die Daten nicht komprimierbar sind.

Type: Long

[BytesTransferred](#)

Die Anzahl der Byte, die vor der Komprimierung an das Netzwerk DataSync gesendet werden (sofern eine Komprimierung möglich ist). Informationen zur Anzahl der über das Netzwerk übertragenen Byte finden Sie unter [BytesCompressed](#).

Type: Long

[BytesWritten](#)

Die Anzahl der logischen Byte, die DataSync tatsächlich an den Zielspeicherort schreiben.

Type: Long

[EndTime](#)

Der Zeitpunkt, zu dem die Übertragungsaufgabe endet.

Typ: Zeitstempel

[EstimatedBytesToTransfer](#)

Die Anzahl der logischen Byte, die DataSync voraussichtlich an den Zielspeicherort geschrieben werden.

Type: Long

[EstimatedFilesToDelete](#)

Die Anzahl der Dateien, Objekte und Verzeichnisse, die DataSync voraussichtlich an Ihrem Zielort gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, [dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle](#) befinden, ist der Wert immer 0.

Note

Bei [Aufgaben im erweiterten Modus](#) umfasst dieser Zähler nur Dateien oder Objekte. Verzeichnisse werden mitgezählt [EstimatedFoldersToDelete](#).

Type: Long

[EstimatedFilesToTransfer](#)

Die Anzahl der Dateien, Objekte und Verzeichnisse, die DataSync voraussichtlich über das Netzwerk übertragen werden. Dieser Wert wird während der DataSync [Vorbereitung](#) der Übertragung berechnet.

Wie dieser Wert berechnet wird, hängt in erster Linie von der Konfiguration des [Übertragungsmodus](#) Ihrer Aufgabe ab:

- Wenn auf gesetzt TransferMode ist CHANGED — Die Berechnung basiert auf dem Vergleich des Inhalts der Quell- und Zielspeicherorte und der Bestimmung der Differenz, die übertragen werden muss. Der Unterschied kann Folgendes beinhalten:
 - Alles, was am Quellspeicherort hinzugefügt oder geändert wurde.
 - Alles, was sich an beiden Speicherorten [OverwriteMode](#) befindet und nach einer ersten Übertragung am Ziel geändert wurde (sofern nicht auf eingestellt NEVER).
 - (Nur einfacher Aufgabenmodus) Die Anzahl der Elemente, die DataSync voraussichtlich gelöscht werden (falls [PreserveDeletedFiles](#) auf gesetzt REMOVE).
- Wenn auf gesetzt TransferMode ist ALL — Die Berechnung basiert nur auf den Elementen, die am DataSync Quellspeicherort gefunden wurden.

Note

Bei [Aufgaben im erweiterten Modus](#) umfasst dieser Leistungsindikator nur Dateien oder Objekte. Verzeichnisse werden mitgezählt [EstimatedFoldersToTransfer](#).

Type: Long

EstimatedFoldersToDelete

Die Anzahl der Verzeichnisse, die DataSync voraussichtlich an Ihrem Zielort gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden, ist der Wert immer 0.

Note

Gilt nur für Aufgaben im erweiterten Modus.

Type: Long

EstimatedFoldersToTransfer

Die Anzahl der Verzeichnisse, die DataSync voraussichtlich über das Netzwerk übertragen werden. Dieser Wert wird berechnet, während die Verzeichnisse für die Übertragung DataSync vorbereitet werden.

Wie dieser Wert berechnet wird, hängt in erster Linie von der Konfiguration des Übertragungsmodus Ihrer Aufgabe ab:

- Wenn auf gesetzt TransferMode ist CHANGED — Die Berechnung basiert auf dem Vergleich des Inhalts der Quell- und Zielspeicherorte und der Bestimmung der Differenz, die übertragen werden muss. Der Unterschied kann Folgendes beinhalten:
 - Alles, was am Quellspeicherort hinzugefügt oder geändert wurde.
 - Alles, was sich an beiden Speicherorten OverwriteMode befindet und nach einer ersten Übertragung am Ziel geändert wurde (sofern nicht auf eingestellt NEVER).
- Wenn auf gesetzt TransferMode ist ALL — Die Berechnung basiert nur auf den Elementen, die am DataSync Quellspeicherort gefunden wurden.

Note

Gilt nur für Aufgaben im erweiterten Modus.

Type: Long

Excludes

Eine Liste von Filterregeln, die bestimmte Daten während Ihrer Übertragung ausschließen. Weitere Informationen und Beispiele finden Sie unter [Filtern von Daten, die übertragen wurden DataSync](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

FilesDeleted

Die Anzahl der Dateien, Objekte und Verzeichnisse, die an Ihrem Zielort DataSync tatsächlich gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, [dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden](#), ist der Wert immer 0.

Note

Bei [Aufgaben im erweiterten Modus](#) umfasst dieser Zähler nur Dateien oder Objekte. Verzeichnisse werden mitgezählt [FoldersDeleted](#).

Typ: Long

FilesFailed

Die Anzahl der Dateien oder Objekte, die DataSync während der Ausführung der Aufgabe nicht vorbereitet, übertragen, verifiziert und gelöscht werden konnten.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Typ: [TaskExecutionFilesFailedDetail](#) Objekt

FilesListed

Die Anzahl der Dateien oder Objekte, die DataSync an Ihren Standorten gefunden wurden.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Typ: [TaskExecutionFilesListedDetail](#) Objekt

[FilesPrepared](#)

Die Anzahl der Dateien oder Objekte, DataSync die nach dem Vergleich Ihrer Quell- und Zielspeicherorte zu übertragen versuchen.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Dieser Zähler gilt nicht, wenn Sie Ihre Aufgabe so konfigurieren, dass [alle Daten übertragen werden](#). In diesem Szenario wird alles von der Quelle zum Ziel DataSync kopiert, ohne die Unterschiede zwischen den Speicherorten zu vergleichen.

Type: Long

[FilesSkipped](#)

Die Anzahl der Dateien, Objekte und Verzeichnisse, die bei der Übertragung DataSync übersprungen werden.

Note

Bei [Aufgaben im erweiterten Modus](#) umfasst dieser Zähler nur Dateien oder Objekte. Verzeichnisse werden mitgezählt [FoldersSkipped](#).

Type: Long

[FilesTransferred](#)

Die Anzahl der Dateien, Objekte und Verzeichnisse, die DataSync tatsächlich über das Netzwerk übertragen werden. Dieser Wert wird während der Ausführung der Aufgabe regelmäßig aktualisiert, wenn etwas aus der Quelle gelesen und über das Netzwerk gesendet wird.

Wenn DataSync etwas nicht übertragen werden kann, kann dieser Wert kleiner als `seinEstimatedFilesToTransfer`. In einigen Fällen kann dieser Wert auch größer als `seinEstimatedFilesToTransfer`. Dieses Element ist für einige Standorttypen implementierungsspezifisch. Verwenden Sie es also nicht, um genau anzugeben, was übertragen wird, oder um die Ausführung Ihrer Aufgabe zu überwachen.

 Note

Bei [Aufgaben im erweiterten Modus](#) umfasst dieser Zähler nur Dateien oder Objekte. Verzeichnisse werden mitgezählt [FoldersTransferred](#).

Type: Long

[FilesVerified](#)

Die Anzahl der Dateien, Objekte und Verzeichnisse, die während der Übertragung DataSync überprüft werden.

 Note

Wenn Sie Ihre Aufgabe so konfigurieren, [dass nur die übertragenen Daten überprüft](#) werden. In manchen Situationen werden Verzeichnisse oder Dateien, die DataSync nicht übertragen werden können, nicht überprüft.

Bei [Aufgaben im erweiterten Modus](#) umfasst dieser Leistungsindikator nur Dateien oder Objekte. Verzeichnisse werden mitgezählt [FoldersVerified](#).

Type: Long

[FoldersDeleted](#)

Die Anzahl der Verzeichnisse, die an Ihrem Zielort DataSync tatsächlich gelöscht werden. Wenn Sie Ihre Aufgabe nicht so konfigurieren, [dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden](#), ist der Wert immer 0.

 Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Type: Long

[FoldersFailed](#)

Die Anzahl der Verzeichnisse, DataSync die während der Ausführung der Aufgabe nicht aufgelistet, vorbereitet, übertragen, überprüft und gelöscht werden können.

 Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Typ: [TaskExecutionFoldersFailedDetail](#) Objekt

[FoldersListed](#)

Die Anzahl der Verzeichnisse, die DataSync an Ihren Standorten gefunden werden.

 Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Typ: [TaskExecutionFoldersListedDetail](#) Objekt

[FoldersPrepared](#)

Die Anzahl der Verzeichnisse, DataSync die nach dem Vergleich Ihrer Quell- und Zielverzeichnisse zu übertragen versuchen.

 Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Dieser Zähler gilt nicht, wenn Sie Ihre Aufgabe so konfigurieren, dass [alle Daten übertragen werden](#). In diesem Szenario wird alles von der Quelle zum Ziel DataSync kopiert, ohne die Unterschiede zwischen den Speicherorten zu vergleichen.

Type: Long

[FoldersSkipped](#)

Die Anzahl der Verzeichnisse, die bei der Übertragung DataSync übersprungen werden.

 Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Type: Long

FoldersTransferred

Die Anzahl der Verzeichnisse, die DataSync tatsächlich über das Netzwerk übertragen werden. Dieser Wert wird während der Ausführung der Aufgabe regelmäßig aktualisiert, wenn etwas aus der Quelle gelesen und über das Netzwerk gesendet wird.

Wenn DataSync etwas nicht übertragen werden kann, kann dieser Wert kleiner als `seinEstimatedFoldersToTransfer`. In einigen Fällen kann dieser Wert auch größer als `seinEstimatedFoldersToTransfer`.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Type: Long

FoldersVerified

Die Anzahl der Verzeichnisse, die während der Übertragung DataSync überprüft werden.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Type: Long

Includes

Eine Liste von Filterregeln, die während der Übertragung bestimmte Daten enthalten. Weitere Informationen und Beispiele finden Sie unter [Filtern von Daten, die übertragen wurden DataSync](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

LaunchTime

Der Zeitpunkt, zu dem die Ausführung der Aufgabe tatsächlich beginnt. Für Aufgaben, die sich nicht in der Warteschlange befinden, `LaunchTime` `StartTime` sind sie in der Regel identisch.

Bei Aufgaben in der Warteschlange `LaunchTime` erfolgt dies in der Regel später, als `StartTime` weil Aufgaben, die zuvor in der Warteschlange standen, erst abgeschlossen werden müssen, bevor neuere Aufgaben beginnen können.

Typ: Zeitstempel

[ManifestConfig](#)

Die Konfiguration des Manifests, das die zu übertragenden Dateien oder Objekte auflistet. Weitere Informationen finden Sie unter [Mithilfe eines Manifests angeben, welche DataSync Übertragungen übertragen](#) werden.

Typ: [ManifestConfig](#) Objekt

[Options](#)

Gibt an, wie Ihre Übertragungsaufgabe konfiguriert ist. Zu diesen Optionen gehört, DataSync wie mit Dateien, Objekten und den zugehörigen Metadaten während der Übertragung umgegangen wird. Sie können unter anderem auch angeben, wie die Datenintegrität überprüft werden soll, Bandbreitenlimits für Ihre Aufgabe festlegen.

Jede Option hat einen Standardwert. Sofern Sie dies nicht möchten, müssen Sie vor dem Aufrufen keine Option konfigurieren [StartTaskExecution](#).

Sie können Ihre Aufgabenoptionen auch für jede Aufgabenausführung überschreiben. Möglicherweise möchten Sie die `LogLevel` für eine einzelne Ausführung anpassen.

Typ: [Options](#) Objekt

[ReportResult](#)

Gibt an, ob ein vollständiger [Aufgabenbericht](#) für Ihre Übertragung DataSync generiert wurde.

Typ: [ReportResult](#) Objekt

[Result](#)

Das Ergebnis der Aufgabenausführung.

Typ: [TaskExecutionResultDetail](#) Objekt

[StartTime](#)

Die Uhrzeit, zu der die Anforderung zum Starten der Aufgabenausführung DataSync gesendet wird. Für Aufgaben, die sich nicht in der Warteschlange befinden, `LaunchTime` `StartTime`

sind sie in der Regel identisch. Bei Aufgaben in der Warteschlange `LaunchTime` erfolgt dies in der Regel später, als `StartTime` weil Aufgaben, die zuvor in der Warteschlange standen, erst abgeschlossen werden müssen, bevor neuere Aufgaben beginnen können.

Typ: Zeitstempel

Status

Der Status der Aufgabenausführung.

Ausführliche Informationen zum Status der Aufgabenausführung finden Sie unter [Status der Aufgabenausführung](#).

Typ: Zeichenfolge

Zulässige Werte: QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING
| VERIFYING | SUCCESS | ERROR

TaskExecutionArn

Der ARN der Aufgabenausführung, über die Sie Informationen benötigen. `TaskExecutionArn` ist hierarchisch und bezieht sich auf `TaskArn` die Aufgabe, die ausgeführt wurde.

Beispielsweise `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2/execution/exec-08ef1e88ec491019b` führte ein `TaskExecution` Wert mit dem ARN die Aufgabe mit dem ARN `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2`.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

TaskMode

Der Aufgabenmodus, den Sie verwenden. Weitere Informationen finden Sie unter [Auswählen eines Aufgabenmodus für Ihre Datenübertragung](#).

Typ: Zeichenfolge

Zulässige Werte: BASIC | ENHANCED

[TaskReportConfig](#)

Die Konfiguration Ihres Aufgabenberichts, der detaillierte Informationen zu Ihrer DataSync Übertragung enthält. Weitere Informationen finden Sie unter [Aufgabenbericht erstellen](#).

Typ: [TaskReportConfig](#) Objekt

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Dieses Beispiel veranschaulicht eine DescribeTaskExecution Anfrage.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccdddf/execution/exec-1234abcd1234abcd1"
}
```

Beispielantwort 1 für die Ausführung einer Aufgabe im erweiterten Modus

Das folgende Beispiel beschreibt eine DataSync Aufgabenausführung, die den erweiterten Modus verwendet. Bei der Ausführung werden auch bestimmte Daten mithilfe von Ausschluss- und Include-Filtern übertragen.

```
{
```

```
"TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddd/execution/exec-1234abcd1234abcd1",
"Status": "SUCCESS",
"Options": {
  "VerifyMode": "ONLY_FILES_TRANSFERRED",
  "OverwriteMode": "ALWAYS",
  "Atime": "BEST_EFFORT",
  "Mtime": "PRESERVE",
  "Uid": "NONE",
  "Gid": "NONE",
  "PreserveDeletedFiles": "PRESERVE",
  "PreserveDevices": "NONE",
  "PosixPermissions": "NONE",
  "BytesPerSecond": -1,
  "TaskQueueing": "ENABLED",
  "LogLevel": "BASIC",
  "TransferMode": "CHANGED",
  "SecurityDescriptorCopyFlags": "NONE",
  "ObjectTags": "PRESERVE"
},
"Excludes": [{
  "FilterType": "SIMPLE_PATTERN",
  "Value": "/archive-files"
}],
"Includes": [{
  "FilterType": "SIMPLE_PATTERN",
  "Value": "/files"
}],
"StartTime": "2024-10-16T11:19:56.844000-04:00",
"EstimatedFilesToTransfer": 7,
"EstimatedFoldersToTransfer": 2,
"EstimatedBytesToTransfer": 30,
"FilesTransferred": 7,
"FoldersTransferred": 2,
"BytesWritten": 30,
"BytesTransferred": 30,
"BytesCompressed": 30,
"Result": {
  "PrepareDuration": 0,
  "PrepareStatus": "SUCCESS",
  "TotalDuration": 3310,
  "TransferDuration": 0,
  "TransferStatus": "SUCCESS",
  "VerifyDuration": 0,
```



```

    "VerifyStatus": "SUCCESS"
  },
  "FilesDeleted": 0,
  "FilesSkipped": 0,
  "FilesVerified": 7,
  "EstimatedFilesToDelete": 0,
  "TaskMode": "ENHANCED",
  "FilesPrepared": 7,
  "FilesListed": {
    "AtSource": 7,
    "AtDestinationForDelete": 0
  },
  "FilesFailed": {
    "Prepare": 0,
    "Transfer": 0,
    "Verify": 0,
    "Delete": 0
  },
  "FoldersDeleted": 0,
  "FoldersSkipped": 0,
  "FoldersVerified": 2,
  "FoldersPrepared": 2,
  "FoldersListed": {
    "AtSource": 2,
    "AtDestinationForDelete": 0
  },
  "FoldersFailed": {
    "List": 0,
    "Prepare": 0,
    "Transfer": 0,
    "Verify": 0,
    "Delete": 0
  }
}

```

Beispielantwort 2 für die Ausführung einer Aufgabe im erweiterten Modus

Das folgende Beispiel beschreibt eine weitere DataSync Aufgabenausführung, die den erweiterten Modus verwendet. In dieser Situation überträgt die Ausführung bestimmte Daten mithilfe eines Manifests anstelle von Filtern.

```
{
```

```

    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddd/execution/exec-1234abcd1234abcd1",
    "Status": "SUCCESS",
    "Options": {
        "VerifyMode": "ONLY_FILES_TRANSFERRED",
        "OverwriteMode": "ALWAYS",
        "Atime": "BEST_EFFORT",
        "Mtime": "PRESERVE",
        "Uid": "NONE",
        "Gid": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "PreserveDevices": "NONE",
        "PosixPermissions": "NONE",
        "BytesPerSecond": -1,
        "TaskQueueing": "ENABLED",
        "LogLevel": "TRANSFER",
        "TransferMode": "CHANGED",
        "SecurityDescriptorCopyFlags": "NONE",
        "ObjectTags": "PRESERVE"
    },
    "Excludes": [],
    "Includes": [],
    "ManifestConfig": {
        "Action": "TRANSFER",
        "Format": "CSV",
        "S3AccessRoleArn": "arn:aws:iam::111222333444:role/service-role/
DataSyncS3ManifestAccess",
        "S3Bucket": "arn:aws:s3:::manifests-datasync",
        "VersionId": "Ixs7NQzEOj8BkL9r4ywX2FtDh_cPf3mG",
        "Source": {
            "S3": {
                "ManifestObjectPath": "manifest-folder/manifest-versioned-files",
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-manifest-
role/DataSyncS3ManifestAccess",
                "S3BucketArn": "arn:aws:s3:::manifests-datasync",
                "ManifestObjectVersionId": "Ixs7NQzEOj8BkL9r4ywX2FtDh_cPf3mG"
            }
        }
    },
    "StartTime": "2024-10-16T09:29:56.757000-04:00",
    "EstimatedFilesToTransfer": 1,
    "EstimatedFoldersToTransfer": 0,
    "EstimatedBytesToTransfer": 6,
    "FilesTransferred": 1,

```

```

"FoldersTransferred": 1,
"BytesWritten": 6,
"BytesTransferred": 6,
"BytesCompressed": 6,
"Result": {
    "PrepareDuration": 0,
    "PrepareStatus": "SUCCESS",
    "TotalDuration": 3089,
    "TransferDuration": 0,
    "TransferStatus": "SUCCESS",
    "VerifyDuration": 0,
    "VerifyStatus": "SUCCESS"
},
"TaskReportConfig": {
    "Destination": {
        "S3": {
            "Subdirectory": "reports/",
            "S3BucketArn": "arn:aws:s3:::my-task-report",
            "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-task-report-
role/DataSyncTaskReportS3BucketAccess"
        }
    },
    "OutputType": "STANDARD",
    "ReportLevel": "SUCSESSES_AND_ERRORS",
    "ObjectVersionIds": "INCLUDE"
},
"FilesDeleted": 0,
"FilesSkipped": 0,
"FilesVerified": 1,
"ReportResult": {
    "Status": "SUCCESS"
},
"EstimatedFilesToDelete": 0,
"TaskMode": "ENHANCED",
"FilesPrepared": 1,
"FilesListed": {
    "AtSource": 1,
    "AtDestinationForDelete": 0
},
"FilesFailed": {
    "Prepare": 0,
    "Transfer": 0,
    "Verify": 0,
    "Delete": 0
}

```

```

    },
    "FoldersDeleted": 0,
    "FoldersSkipped": 0,
    "FoldersVerified": 0,
    "FoldersPrepared": 0,
    "FoldersListed": {
        "AtSource": 0,
        "AtDestinationForDelete": 0
    },
    "FoldersFailed": {
        "List": 0,
        "Prepare": 0,
        "Transfer": 0,
        "Verify": 0,
        "Delete": 0
    }
}

```

Beispielantwort für die Ausführung einer Aufgabe im Basismodus

Das folgende Beispiel beschreibt eine DataSync Aufgabenausführung, die den Basismodus verwendet.

```

{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccdddf/execution/exec-1234abcd1234abcd1",
    "BytesCompressed": 3500,
    "BytesTransferred": 5000,
    "BytesWritten": 5000,
    "EstimatedBytesToTransfer": 5000,
    "EstimatedFilesToDelete": 10,
    "EstimatedFilesToTransfer": 100,
    "FilesDeleted": 10,
    "FilesSkipped": 0,
    "FilesTransferred": 100,
    "FilesVerified": 100,
    "Result": {
        "PrepareDuration": 100,
        "PrepareStatus": "SUCCESS",
        "TransferDuration": 60,
        "TransferStatus": "SUCCESS",
        "VerifyDuration": 30,
        "VerifyStatus": "SUCCESS"
    }
}

```

```

    },
    "StartTime": "2024-10-16T11:19:56.844000-04:00",
    "Status": "SUCCESS",
    "OverrideOptions": {
        "Atime": "BEST_EFFORT",
        "BytesPerSecond": "1000",
        "Gid": "NONE",
        "Mtime": "PRESERVE",
        "PosixPermissions": "PRESERVE",
        "PreserveDeletedFiles": "PRESERVE",
        "Uid": "NONE",
        "VerifyMode": "POINT_IN_TIME_CONSISTENT"
    },
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-datasync-
role",
                "S3BucketArn": "arn:aws:s3:::my-task-reports-bucket/*",
                "Subdirectory": "reports"
            }
        },
        "ObjectVersionIds": "INCLUDE",
        "OutputType": "STANDARD",
        "Overrides": {
            "Deleted": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Skipped": {
                "ReportLevel": "SUCCESSSES_AND_ERRORS"
            },
            "Transferred": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Verified": {
                "ReportLevel": "ERRORS_ONLY"
            }
        },
        "ReportLevel": "ERRORS_ONLY"
    }
}

```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListAgents

Gibt eine Liste von AWS DataSync Agenten zurück, die zu einem AWS-Konto in der Anfrage AWS-Region angegebenen gehören.

Mit der Paginierung können Sie die Anzahl der Agenten reduzieren, die in einer Antwort zurückgegeben werden. Wenn Sie in einer Antwort eine gekürzte Liste von Agenten erhalten, enthält die Antwort eine Markierung, die Sie in Ihrer nächsten Anfrage angeben können, um die nächste Agentenseite abzurufen.

ListAgents ist letztlich konsistent. Das bedeutet, dass das Ergebnis der Ausführung des Vorgangs möglicherweise nicht darauf hindeutet, dass Sie gerade einen Agenten erstellt oder gelöscht haben. Wenn Sie beispielsweise einen Agenten mit erstellen [CreateAgent](#) und ihn dann sofort ausführen ListAgents, wird dieser Agent möglicherweise nicht sofort in der Liste angezeigt. In solchen Situationen können Sie jederzeit überprüfen, ob ein Agent erstellt (oder gelöscht) wurde, indem Sie [DescribeAgent](#)

Anforderungssyntax

```
{  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[MaxResults](#)

Gibt die maximale Anzahl von DataSync Agenten an, die in einer Antwort aufgeführt werden sollen. Standardmäßig werden in einer Antwort maximal 100 Agenten angezeigt.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximalwert 100.

Erforderlich: Nein

NextToken

Gibt eine undurchsichtige Zeichenfolge an, die die Position angibt, an der die nächste Ergebnisliste in der Antwort beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Erforderlich: Nein

Antwortsyntax

```
{
  "Agents": [
    {
      "AgentArn": "string",
      "Name": "string",
      "Platform": {
        "Version": "string"
      },
      "Status": "string"
    }
  ],
  "NextToken": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Agents

Eine Liste der DataSync Agenten in Ihrem Namen, wie AWS-Konto in der AWS-Region Anfrage angegeben. Die Liste ist nach den Amazon-Ressourcennamen der Agenten (ARNs) sortiert.

Typ: Array von AgentListEntry-Objekten

NextToken

Die undurchsichtige Zeichenfolge, die die Position angibt, an der die nächste Ergebnisliste in der Antwort beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im Dienst ein Fehler auftritt. AWS DataSync

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListLocations

Gibt eine Liste von Quell- und Zielorten zurück.

Wenn Sie mehr Standorte haben, als in einer Antwort zurückgegeben werden (d. h., die Antwort gibt nur eine gekürzte Liste Ihrer Agenten zurück), enthält die Antwort ein Token, das Sie in Ihrer nächsten Anfrage angeben können, um die nächste Seite mit Standorten abzurufen.

Anforderungssyntax

```
{
  "Filters": [
    {
      "Name": "string",
      "Operator": "string",
      "Values": [ "string" ]
    }
  ],
  "MaxResults": number,
  "NextToken": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[Filters](#)

Sie können API-Filter verwenden, um die Liste der von zurückgegebenen Ressourcen einzugrenzen. `ListLocations` Um beispielsweise alle Aufgaben an einem bestimmten Quellspeicherort abzurufen, können Sie `ListLocations` with filter name `LocationType` `S3` and verwenden `Operator` `Equals`.

Typ: Array von [LocationFilter](#)-Objekten

Erforderlich: Nein

[MaxResults](#)

Die maximale Anzahl von Standorten, die zurückgegeben werden sollen.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximalwert 100.

Erforderlich: Nein

[NextToken](#)

Eine undurchsichtige Zeichenfolge, die die Position angibt, an der die nächste Liste von Orten beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Erforderlich: Nein

Antwortsyntax

```
{
  "Locations": [
    {
      "LocationArn": "string",
      "LocationUri": "string"
    }
  ],
  "NextToken": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[Locations](#)

Ein Array, das eine Liste von Orten enthält.

Typ: Array von [LocationListEntry](#)-Objekten

NextToken

Eine undurchsichtige Zeichenfolge, die die Position angibt, an der mit der Rückgabe der nächsten Ortsliste begonnen werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im Dienst ein Fehler auftritt. AWS DataSync

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListTagsForResource

Gibt alle mit einer AWS Ressource verknüpften Tags zurück.

Anforderungssyntax

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "ResourceArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[MaxResults](#)

Gibt an, wie viele Ergebnisse die Antwort enthalten soll.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximalwert 100.

Erforderlich: Nein

[NextToken](#)

Gibt eine undurchsichtige Zeichenfolge an, die die Position angibt, an der die nächste Ergebnisliste in der Antwort beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Erforderlich: Nein

[ResourceArn](#)

Gibt den Amazon-Ressourcennamen (ARN) der Ressource an, für die Sie Tag-Informationen wünschen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:(((agent|task|location)/(agent|task|loc)-[a-z0-9]{17}(/execution/exec-[a-f0-9]{17})?)|(system/storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}(/job/discovery-job-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})?)))$`

Erforderlich: Ja

Antwortsyntax

```
{
  "NextToken": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[NextToken](#)

Die undurchsichtige Zeichenfolge, die die Position angibt, an der die nächste Ergebnisliste in der Antwort beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Tags

Eine Reihe von Tags, die auf die angegebene Ressource angewendet wurden.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Maximale Anzahl von 55 Elementen.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)

- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

ListTaskExecutions

Gibt eine Liste von Ausführungen für eine AWS DataSync Übertragungsaufgabe zurück.

Anforderungssyntax

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "TaskArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[MaxResults](#)

Gibt an, wie viele Ergebnisse die Antwort enthalten soll.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximalwert 100.

Erforderlich: Nein

[NextToken](#)

Gibt eine undurchsichtige Zeichenfolge an, die die Position angibt, an der die nächste Ergebnisliste in der Antwort beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Erforderlich: Nein

[TaskArn](#)

Gibt den Amazon-Ressourcennamen (ARN) der Aufgabe an, zu der Sie Ausführungsinformationen benötigen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erforderlich: Nein

Antwortsyntax

```
{
  "NextToken": "string",
  "TaskExecutions": [
    {
      "Status": "string",
      "TaskExecutionArn": "string",
      "TaskMode": "string"
    }
  ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[NextToken](#)

Die undurchsichtige Zeichenfolge, die die Position angibt, an der die nächste Ergebnisliste in der Antwort beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

[TaskExecutions](#)

Eine Liste der Ausführungen der Aufgabe.

Typ: Array von [TaskExecutionListEntry](#)-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)

- [AWS SDK for Ruby V3](#)

ListTasks

Gibt eine Liste der AWS DataSync Aufgaben zurück, die Sie erstellt haben.

Anforderungssyntax

```
{
  "Filters": [
    {
      "Name": "string",
      "Operator": "string",
      "Values": [ "string" ]
    }
  ],
  "MaxResults": number,
  "NextToken": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[Filters](#)

Sie können API-Filter verwenden, um die Liste der von zurückgegebenen Ressourcen einzugrenzen `ListTasks`. Um beispielsweise alle Aufgaben an einem bestimmten Quellspeicherort abzurufen, können Sie dies `ListTasks` mit dem Filternamen `LocationId` und `Operator Equals` mit dem ARN für den Speicherort verwenden.

Typ: Array von [TaskFilter](#)-Objekten

Erforderlich: Nein

[MaxResults](#)

Die maximale Anzahl von Aufgaben, die zurückgegeben werden sollen.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 0. Maximalwert 100.

Erforderlich: Nein

[NextToken](#)

Eine undurchsichtige Zeichenfolge, die die Position angibt, an der die nächste Aufgabenliste beginnen soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

Erforderlich: Nein

Antwortsyntax

```
{
  "NextToken": "string",
  "Tasks": [
    {
      "Name": "string",
      "Status": "string",
      "TaskArn": "string",
      "TaskMode": "string"
    }
  ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

[NextToken](#)

Eine undurchsichtige Zeichenfolge, die die Position angibt, an der mit der Rückgabe der nächsten Aufgabenliste begonnen werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 65535.

Pattern: [a-zA-Z0-9=_-]+

[Tasks](#)

Eine Liste aller zurückgegebenen Aufgaben.

Typ: Array von [TaskListEntry](#)-Objekten

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)

- [AWS SDK for Ruby V3](#)

StartTaskExecution

Startet eine AWS DataSync Übertragungsaufgabe. Für jede Aufgabe können Sie jeweils nur eine Aufgabenausführung ausführen.

Die Ausführung einer Aufgabe besteht aus mehreren Schritten. Weitere Informationen finden Sie unter [Status der Aufgabenausführung](#).

Important

Wenn Sie planen, Daten zu oder von einem Amazon S3 S3-Standort zu übertragen, lesen Sie zunächst, [wie sich dies auf Ihre S3-Anforderungsgebühren auswirken DataSync kann](#), sowie auf der [DataSync Preisseite](#).

Anforderungssyntax

```
{
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
      }
    }
  }
},
```

```

"OverrideOptions": {
  "Atime": "string",
  "BytesPerSecond": number,
  "Gid": "string",
  "LogLevel": "string",
  "Mtime": "string",
  "ObjectTags": "string",
  "OverwriteMode": "string",
  "PosixPermissions": "string",
  "PreserveDeletedFiles": "string",
  "PreserveDevices": "string",
  "SecurityDescriptorCopyFlags": "string",
  "TaskQueueing": "string",
  "TransferMode": "string",
  "Uid": "string",
  "VerifyMode": "string"
},
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"TaskArn": "string",
"TaskReportConfig": {
  "Destination": {
    "S3": {
      "BucketAccessRoleArn": "string",
      "S3BucketArn": "string",
      "Subdirectory": "string"
    }
  },
  "ObjectVersionIds": "string",
  "OutputType": "string",
  "Overrides": {
    "Deleted": {
      "ReportLevel": "string"
    },
    "Skipped": {
      "ReportLevel": "string"
    },
    "Transferred": {
      "ReportLevel": "string"
    }
  },

```

```
    "Verified": {  
      "ReportLevel": "string"  
    },  
    "ReportLevel": "string"  
  }  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[Excludes](#)

Gibt eine Liste von Filterregeln an, die bestimmt, welche Dateien von einer Aufgabe ausgeschlossen werden sollen. Die Liste enthält eine einzelne Filterzeichenfolge, die aus den auszuschließenden Mustern besteht. Die Muster werden durch "|" (also eine Pipe) abgegrenzt. Beispiel: `"/folder1|/folder2"`.

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

Erforderlich: Nein

[Includes](#)

Gibt eine Liste von Filterregeln an, die bestimmt, welche Dateien bei der Ausführung einer Aufgabe berücksichtigt werden sollen. Das Muster sollte eine einzelne Filterzeichenfolge enthalten, die aus den einzuschließenden Mustern besteht. Die Muster werden durch "|" (also eine Pipe) abgegrenzt. Beispiel: `"/folder1|/folder2"`.

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

Erforderlich: Nein

ManifestConfig

Konfiguriert ein Manifest, bei dem es sich um eine Liste von Dateien oder Objekten handelt, die Sie übertragen DataSync möchten. Weitere Informationen und Konfigurationsbeispiele finden Sie unter [Mithilfe eines Manifests angeben, was DataSync übertragen werden soll](#).

Wenn Sie diesen Parameter verwenden, muss Ihre Anruferidentität (die Rolle, DataSync mit der Sie ihn verwenden) über die `iam:PassRole` entsprechende Berechtigung verfügen. Die [AWSDataSyncFullAccess](#) Richtlinie beinhaltet diese Erlaubnis.

Um eine Manifestkonfiguration zu entfernen, geben Sie diesen Parameter mit einem leeren Wert an.

Typ: [ManifestConfig](#) Objekt

Erforderlich: Nein

OverrideOptions

Gibt an, wie Ihre Übertragungsaufgabe konfiguriert ist. Zu diesen Optionen gehört, DataSync wie mit Dateien, Objekten und den zugehörigen Metadaten während der Übertragung umgegangen wird. Sie können unter anderem auch angeben, wie die Datenintegrität überprüft werden soll, Bandbreitenlimits für Ihre Aufgabe festlegen.

Jede Option hat einen Standardwert. Sofern Sie dies nicht möchten, müssen Sie vor dem Aufrufen keine Option konfigurieren [StartTaskExecution](#).

Sie können Ihre Aufgabenoptionen auch für jede Aufgabenausführung überschreiben. Möglicherweise möchten Sie die `LogLevel` für eine einzelne Ausführung anpassen.

Typ: [Options](#) Objekt

Erforderlich: Nein

Tags

Gibt die Tags an, die Sie auf den Amazon-Ressourcennamen (ARN) anwenden möchten, der die Aufgabenausführung darstellt.

Tags sind Schlüssel-Wert-Paare, die Ihnen helfen, Ihre DataSync Ressourcen zu verwalten, zu filtern und nach ihnen zu suchen.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Nein

TaskArn

Gibt den Amazon-Ressourcennamen (ARN) der Aufgabe an, die Sie starten möchten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erforderlich: Ja

TaskReportConfig

Gibt an, wie Sie einen Aufgabenbericht konfigurieren möchten, der detaillierte Informationen zu Ihrer DataSync Übertragung enthält. Weitere Informationen finden Sie unter [Überwachen Ihrer DataSync Übertragungen mit Aufgabenberichten](#).

Wenn Sie diesen Parameter verwenden, muss Ihre Anruferidentität (die Rolle, DataSync mit der Sie ihn verwenden) über die `iam:PassRole` entsprechende Berechtigung verfügen. Die [AWSDataSyncFullAccess](#) Richtlinie beinhaltet diese Erlaubnis.

Um eine Task-Berichtskonfiguration zu entfernen, geben Sie diesen Parameter als leer an.

Typ: [TaskReportConfig](#) Objekt

Erforderlich: Nein

Antwortsyntax

```
{
  "TaskExecutionArn": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

TaskExecutionArn

Der ARN der Ausführung der laufenden Aufgabe.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Beispiele

Beispielanforderung

Im folgenden Beispiel wird eine Aufgabenausführung mit den Standardoptionen für die angegebene Aufgabe gestartet.

```
{
  "OverrideOptions": {
    "Atime": "BEST_EFFORT",
    "BytesPerSecond": 1000,
```



```
    "Gid": "NONE",
    "Mtime": "PRESERVE",
    "PosixPermissions": "PRESERVE",
    "PreserveDevices": "NONE",
    "PreserveDeletedFiles": "PRESERVE",
    "Uid": "NONE",
    "VerifyMode": "POINT_IN_TIME_CONSISTENT"
  },
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Beispielantwort

Dieses Beispiel veranschaulicht eine Verwendung von StartTaskExecution.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

TagResource

Wendet ein Tag auf eine AWS Ressource an. Tags sind Schlüssel-Wert-Paare, die Ihnen helfen können, Ihre Ressourcen zu verwalten, zu filtern und nach ihnen zu suchen.

Dazu gehören AWS DataSync Ressourcen wie Standorte, Aufgaben und Aufgabenausführungen.

Anforderungssyntax

```
{
  "ResourceArn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[ResourceArn](#)

Gibt den Amazon-Ressourcennamen (ARN) der Ressource an, auf die das Tag angewendet werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:(((agent|task|location)/(agent|task|loc)-[a-z0-9]{17}(/execution/exec-[a-f0-9]{17}))?|(system/storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}(/job/discovery-job-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}))?))$`

Erforderlich: Ja

Tags

Gibt die Tags an, die Sie auf die Ressource anwenden möchten.

Typ: Array von [TagListEntry](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente.

Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UntagResource

Entfernt Tags aus einer AWS Ressource.

Anforderungssyntax

```
{  
  "Keys": [ "string" ],  
  "ResourceArn": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Keys

Gibt die Schlüssel in den Tags an, die Sie entfernen möchten.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 50 Elemente.

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:/-]+$`

Erforderlich: Ja

ResourceArn

Gibt den Amazon-Ressourcennamen (ARN) der Ressource an, aus der die Tags entfernt werden sollen.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: ^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:(((agent|task|location)/(agent|task|loc)-[a-z0-9]{17}/execution/exec-[a-f0-9]{17}))?|(system/storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}(/job/discovery-job-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}))?))\$

Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)

- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateAgent

Aktualisiert den Namen eines AWS DataSync Agenten.

Anforderungssyntax

```
{  
  "AgentArn": "string",  
  "Name": "string"  
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AgentArn](#)

Der Amazon-Ressourcenname (ARN) des zu aktualisierenden Agenten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Ja

[Name](#)

Der Name, den Sie zur Konfiguration des Agenten verwenden möchten.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationAzureBlob

Ändert die folgenden Konfigurationen des Microsoft Azure Blob Storage-Übertragungsorts, den Sie mit verwenden. AWS DataSync

Weitere Informationen finden Sie unter [Konfiguration von DataSync Übertragungen mit Azure Blob Storage](#).

Anforderungssyntax

```
{
  "AccessTier": "string",
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlobType": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "LocationArn": "string",
  "SasConfiguration": {
    "Token": "string"
  },
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AccessTier](#)

Gibt die Zugriffsebene an, in die Ihre Objekte oder Dateien übertragen werden sollen. Dies gilt nur, wenn der Standort als Übertragungsziel verwendet wird. Weitere Informationen finden Sie unter [Zugriffsebenen](#).

Typ: Zeichenfolge

Zulässige Werte: HOT | COOL | ARCHIVE

Erforderlich: Nein

[AgentArns](#)

(Optional) Gibt den Amazon-Ressourcennamen (ARN) des DataSync Agenten an, der eine Verbindung mit Ihrem Azure Blob Storage-Container herstellen kann. Wenn Sie eine cloudübergreifende Übertragung ohne Agenten einrichten, müssen Sie für diesen Parameter keinen Wert angeben.

Sie können mehr als einen Agenten angeben. Weitere Informationen finden Sie unter [Mehrere Agenten für Ihre Übertragung verwenden](#).

Note

Sie können keine Agenten zu einem Speicherort hinzufügen oder daraus entfernen, nachdem Sie ihn ursprünglich erstellt haben.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

[AuthenticationType](#)

Gibt die Authentifizierungsmethode an, die für den Zugriff auf Ihren Azure Blob Storage DataSync verwendet wird. DataSync kann mithilfe einer Shared Access Signature (SAS) auf Blob-Speicher zugreifen.

Typ: Zeichenfolge

Zulässige Werte: SAS | NONE

Erforderlich: Nein

BlobType

Gibt den Blobtyp an, den Ihre Objekte oder Dateien haben sollen, wenn sie in Azure Blob Storage übertragen werden. Unterstützt derzeit DataSync nur das Verschieben von Daten in Azure Blob Storage als Blockblobs. Weitere Informationen zu Blobtypen finden Sie in der [Azure Blob Storage](#)-Dokumentation.

Typ: Zeichenfolge

Zulässige Werte: BLOCK

Erforderlich: Nein

CmkSecretConfig

Gibt Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis an, z. B. ein Authentifizierungstoken oder einen Satz von Anmeldeinformationen, das für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet wird, und für einen vom Kunden verwalteten Schlüssel. AWS KMS key

Typ: [CmkSecretConfig](#) Objekt

Erforderlich: Nein

CustomSecretConfig

Gibt Konfigurationsinformationen für ein vom Kunden verwaltetes Geheimnis an, z. B. ein Authentifizierungstoken oder einen Satz von Anmeldeinformationen, das für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet wird, und für ein vom Kunden verwaltetes Geheimnis. AWS KMS key

Typ: [CustomSecretConfig](#) Objekt

Erforderlich: Nein

LocationArn

Gibt den ARN des Azure Blob Storage-Übertragungsorts an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

SasConfiguration

Gibt die SAS-Konfiguration an, die DataSync den Zugriff auf Ihren Azure Blob Storage ermöglicht.

Typ: [AzureBlobSasConfiguration](#) Objekt

Erforderlich: Nein

Subdirectory

Gibt Pfadsegmente an, wenn Sie Ihre Übertragung auf ein virtuelles Verzeichnis in Ihrem Container beschränken möchten (z. B. /my/images).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 1 024.

Pattern: `^[\\p{L}\\p{M}\\p{Z}\\p{S}\\p{N}\\p{P}\\p{C}]*$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationEfs

Ändert die folgenden Konfigurationsparameter des Amazon EFS-Übertragungsorts, den Sie mit AWS DataSync verwenden.

Weitere Informationen finden Sie unter [Konfiguration von DataSync Übertragungen mit Amazon EFS](#).

Anforderungssyntax

```
{
  "AccessPointArn": "string",
  "FileSystemAccessRoleArn": "string",
  "InTransitEncryption": "string",
  "LocationArn": "string",
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AccessPointArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des Access Points an, der zum Mounten Ihres Amazon EFS-Dateisystems DataSync verwendet wird.

Weitere Informationen finden Sie unter [Zugreifen auf eingeschränkte Amazon EFS-Dateisysteme](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: (^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}\$)|(^\$)

Erforderlich: Nein

FileSystemAccessRoleArn

Gibt eine AWS Identity and Access Management (IAM-) Rolle an, die DataSync den Zugriff auf Ihr Amazon EFS-Dateisystem ermöglicht.

Informationen zum Erstellen dieser Rolle finden Sie unter [Erstellen einer DataSync IAM-Rolle für den Zugriff auf das Amazon EFS-Dateisystem](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `(^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$)|(^$)`

Erforderlich: Nein

InTransitEncryption

Gibt an, ob Sie DataSync die Transport Layer Security (TLS) 1.2-Verschlüsselung verwenden möchten, wenn Daten zu oder von Ihrem Amazon EFS-Dateisystem übertragen werden.

Wenn Sie einen Zugriffspunkt mit `AccessPointArn` oder eine IAM-Rolle mit `FileSystemAccessRoleArn` angeben, müssen Sie diesen Parameter auf `TLS1_2` setzen.

Typ: Zeichenfolge

Zulässige Werte: `NONE` | `TLS1_2`

Erforderlich: Nein

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des Amazon EFS-Übertragungsorts an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

[Subdirectory](#)

Gibt einen Mount-Pfad für Ihr Amazon-EFS-Dateisystem an. Hier werden Daten in Ihrem Dateisystem DataSync gelesen oder geschrieben (je nachdem, ob es sich um einen Quell- oder Zielort handelt).

DataSync verwendet standardmäßig das Stammverzeichnis (oder den [Zugriffspunkt](#), falls Sie eines mit `accessPointArn` angeben). Sie können Unterverzeichnisse auch mit Schrägstrichen einbeziehen (z. B. `/path/to/folder`).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\+\.\(\)\p{Zs}]*$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationFsxLustre

Ändert die folgenden Konfigurationsparameter des Amazon FSx for Lustre-Übertragungsorts, den Sie mit verwenden. AWS DataSync

Weitere Informationen finden Sie unter [Konfiguration von DataSync Übertragungen mit FSx for Lustre](#).

Anforderungssyntax

```
{
  "LocationArn": "string",
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[LocationArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des FSx for Lustre-Transferstandorts an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

[Subdirectory](#)

Gibt einen Bereitstellungspfad für Ihr FSx for Lustre-Dateisystem an. Der Pfad kann Unterverzeichnisse enthalten.

Wenn der Speicherort als Quelle verwendet wird, DataSync liest Daten aus dem Mount-Pfad. Wenn der Speicherort als Ziel verwendet wird, werden Daten in den Bereitstellungspfad

DataSync geschrieben. Wenn Sie diesen Parameter nicht angeben, DataSync verwendet das Stammverzeichnis des Dateisystems (/).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationFsxOntap

Ändert die folgenden Konfigurationsparameter des Amazon FSx for NetApp ONTAP-Übertragungsorts, den Sie mit verwenden. AWS DataSync

Weitere Informationen finden Sie unter [DataSyncÜbertragungen konfigurieren mit FSx für ONTAP](#).

Anforderungssyntax

```
{
  "LocationArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des FSx für ONTAP übertragenden Standorts an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Protocol

Gibt das Datenübertragungsprotokoll an, das für den Zugriff auf Ihr FSx Amazon-Dateisystem DataSync verwendet wird.

Typ: [FsxUpdateProtocol](#) Objekt

Erforderlich: Nein

Subdirectory

Gibt einen Pfad zur Dateifreigabe in der virtuellen Speichermaschine (SVM) an, zu der oder von der Sie Daten übertragen möchten.

Sie können einen Knotenpfad (auch als Mount-Punkt bezeichnet), einen Qtree-Pfad (für NFS-Dateifreigaben) oder einen Share-Namen (für SMB-Dateifreigaben) angeben. Ihr Mount-Pfad könnte zum Beispiel `/vol1`, `/vol1/tree1` oder `/share1` sein.

Note

Geben Sie keinen Verbindungspfad im Stammvolume der SVM an. Weitere Informationen finden Sie unter [Verwaltung FSx virtueller ONTAP-Speichermaschinen](#) im Amazon FSx for NetApp ONTAP-Benutzerhandbuch.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im Service ein Fehler auftritt. AWS DataSync

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationFsxOpenZfs

Ändert die folgenden Konfigurationsparameter des Amazon FSx for OpenZFS-Übertragungsorts, den Sie mit verwenden. AWS DataSync

Weitere Informationen finden Sie unter [DataSyncÜbertragungen konfigurieren mit FSx](#) für OpenZFS.

Note

Anforderungsparameter, die sich auf beziehen, werden von dem UpdateLocationFsxOpenZfs Vorgang SMB nicht unterstützt.

Anforderungssyntax

```
{
  "LocationArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

LocationArn

Gibt den Amazon-Ressourcennamen (ARN) des FSx für OpenZFS übertragenen Speicherorts an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Protocol

Gibt das Datenübertragungsprotokoll an, das für den Zugriff auf Ihr FSx Amazon-Dateisystem AWS DataSync verwendet wird.

Typ: [FsxProtocol](#) Objekt

Erforderlich: Nein

Subdirectory

Gibt ein Unterverzeichnis im Pfad des Speicherorts an, das mit /fsx beginnen muss. DataSync verwendet dieses Unterverzeichnis zum Lesen oder Schreiben von Daten (je nachdem, ob es sich bei dem Dateisystem um einen Quell- oder Zielspeicherort handelt).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\+\.\^(\)\$\p{Zs}]+$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationFsxWindows

Ändert die folgenden Konfigurationsparameter des Amazon FSx for Windows File Server-Übertragungsorts, den Sie mit AWS DataSync verwenden.

Weitere Informationen finden Sie unter [Konfiguration von DataSync Übertragungen mit FSx für Windows File Server](#).

Anforderungssyntax

```
{
  "Domain": "string",
  "LocationArn": "string",
  "Password": "string",
  "Subdirectory": "string",
  "User": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[Domain](#)

Gibt den Namen der Windows-Domäne an, zu der Ihr Dateisystem FSx für Windows File Server gehört.

Wenn Sie mehrere Active Directory-Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen Dateisystem hergestellt wird.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}?\\$`

Erforderlich: Nein

LocationArn

Gibt den ARN des Übertragungsorts FSx für den Windows-Dateiserver an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

Password

Gibt das Kennwort des Benutzers an, der berechtigt ist, die Dateien, Ordner und Dateimetadaten in Ihrem Dateisystem FSx für Windows File Server bereitzustellen und darauf zuzugreifen.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^.{0,104}$`

Erforderlich: Nein

Subdirectory

Gibt einen Einhängpfad für Ihr Dateisystem mit Schrägstrichen an. DataSync verwendet dieses Unterverzeichnis zum Lesen oder Schreiben von Daten (je nachdem, ob das Dateisystem ein Quell- oder Zielverzeichnis ist).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\+\.\^(\)\$\\p{Zs}]+$`

Erforderlich: Nein

User

Gibt den Benutzer an, der berechtigt ist, die Dateien, Ordner und Dateimetadaten in Ihrem Dateisystem FSx für Windows File Server bereitzustellen und darauf zuzugreifen.

Informationen zur Auswahl eines Benutzers mit der richtigen Zugriffsebene für Ihre Übertragung finden Sie unter [Erforderliche Berechtigungen](#) FSx für Windows-Dateiserverstandorte.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E]{1,104}$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationHdfs

Ändert die folgenden Konfigurationsparameter des Hadoop Distributed File System (HDFS) - Übertragungsorts, den Sie mit verwenden. AWS DataSync

Weitere Informationen finden Sie unter [Konfiguration von DataSync Übertragungen mit einem HDFS-Cluster](#).

Anforderungssyntax

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlockSize": number,
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "KmsKeyProviderUri": "string",
  "LocationArn": "string",
  "NameNodes": [
    {
      "Hostname": "string",
      "Port": number
    }
  ],
  "QopConfiguration": {
    "DataTransferProtection": "string",
    "RpcProtection": "string"
  },
  "ReplicationFactor": number,
  "SimpleUser": "string",
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AgentArns](#)

Die Amazon-Ressourcennamen (ARNs) der DataSync Agenten, die eine Verbindung zu Ihrem HDFS-Cluster herstellen können.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

[AuthenticationType](#)

Die Art der Authentifizierung, die verwendet wird, um die Identität des Benutzers zu ermitteln.

Typ: Zeichenfolge

Zulässige Werte: SIMPLE | KERBEROS

Erforderlich: Nein

[BlockSize](#)

Die Größe der Datenblöcke, die in den HDFS-Cluster geschrieben werden sollen.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert von 1048576. Der Höchstwert ist 1073741824.

Erforderlich: Nein

[KerberosKeytab](#)

Die Kerberos-Schlüsseltabelle (keytab), die Zuweisungen zwischen dem definierten Kerberos-Prinzipal und den verschlüsselten Schlüsseln enthält. Sie können den Keytab aus einer Datei laden, indem Sie die Adresse der Datei angeben.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 65536.

Erforderlich: Nein

[KerberosKrb5Conf](#)

Die `krb5.conf`-Datei, die die Kerberos-Konfigurationsinformationen enthält. Sie können die `krb5.conf` Datei laden, indem Sie die Adresse der Datei angeben. Wenn Sie das verwenden AWS CLI, führt es die Base64-Kodierung für Sie durch. Andernfalls geben Sie den Base64-codierten Text an.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 131072.

Erforderlich: Nein

[KerberosPrincipal](#)

Das Kerberos-Prinzipal mit Zugriff auf die Dateien und Ordner im HDFS-Cluster.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^\.+`

Erforderlich: Nein

[KmsKeyProviderUri](#)

Die URI des Key Management Servers (KMS) des HDFS-Clusters.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Pattern: `^kms:\\\\http[s]?@(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9])(;(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9]))*:[0-9]{1,5}\\kms$`

Erforderlich: Nein

[LocationArn](#)

Der Amazon-Ressourcenname (ARN) des Quell-HDFS-Cluster-Speicherorts.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

NameNodes

Der NameNode , der den HDFS-Namespace verwaltet. Der NameNode führt Operationen wie das Öffnen, Schließen und Umbenennen von Dateien und Verzeichnissen aus. Das NameNode enthält die Informationen zum Zuordnen von Datenblöcken zu. DataNodes Sie können nur einen verwenden NameNode.

Typ: Array von [HdfsNameNode](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element.

Erforderlich: Nein

QopConfiguration

Die Konfiguration der Quality of Protection (QOP, Schutzqualität) legt den Remote Procedure Call (RPC, Remoteprozeduraufruf) und die Datenschutzeinstellungen für die Datenübertragung fest, die auf dem Hadoop Distributed File System (HDFS)-Cluster konfiguriert sind.

Typ: [QopConfiguration](#) Objekt

Erforderlich: Nein

ReplicationFactor

Die Nummer DataNodes , auf die die Daten repliziert werden sollen, wenn in den HDFS-Cluster geschrieben wird.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Der Maximalwert ist 512.

Erforderlich: Nein

SimpleUser

Der zur Identifizierung des Clients auf dem Host-Betriebssystem verwendete Benutzername.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[_ .A-Za-z0-9][_ .A-Za-z0-9]*$`

Erforderlich: Nein

[Subdirectory](#)

Ein Unterverzeichnis im HDFS-Cluster. Dieses Unterverzeichnis wird verwendet, um Daten vom HDFS-Cluster zu lesen oder zu schreiben.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationNfs

Ändert die folgenden Konfigurationsparameter des NFS-Übertragungsorts (Network File System), den Sie mit verwenden. AWS DataSync

Weitere Informationen finden Sie unter [Konfiguration von Übertragungen mit einem NFS-Dateiserver](#).

Anforderungssyntax

```
{
  "LocationArn": "string",
  "MountOptions": {
    "Version": "string"
  },
  "OnPremConfig": {
    "AgentArns": [ "string" ]
  },
  "ServerHostname": "string",
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[LocationArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des NFS-Übertragungsorts an, den Sie aktualisieren möchten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

MountOptions

Gibt an, wie DataSync mithilfe des NFS-Protokolls auf einen Standort zugegriffen werden kann.

Typ: [NfsMountOptions](#) Objekt

Erforderlich: Nein

OnPremConfig

Die AWS DataSync Agenten, die eine Verbindung zu Ihrem NFS-Dateiserver (Network File System) herstellen können.

Typ: [OnPremConfig](#) Objekt

Erforderlich: Nein

ServerHostname

Gibt den DNS-Namen oder die IP-Adresse (IPv4 oder IPv6) des NFS-Dateiservers an, mit dem Ihr DataSync Agent eine Verbindung herstellt.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^(( [a-zA-Z0-9\ - ]*[a-zA-Z0-9])\ . )*( [A-Za-z0-9\ - : ]*[A-Za-z0-9])$`

Erforderlich: Nein

Subdirectory

Gibt den Exportpfad auf Ihrem NFS-Dateiserver an, den Sie mounten DataSync möchten.

Dieser Pfad (oder ein Unterverzeichnis des Pfads) ist der Ort, an den Daten DataSync übertragen werden oder von diesem Pfad. Informationen zur Konfiguration eines Exports für DataSync finden Sie unter [Zugreifen auf NFS-Dateiserver](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\ -\ +\ .\ /\ (\)\ \p{Zs}]+$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationObjectStorage

Ändert die folgenden Konfigurationsparameter des Objektspeicher-Übertragungsorts, den Sie mit AWS DataSync verwenden.

Weitere Informationen finden Sie unter [Konfiguration von DataSync Übertragungen mit einem Objektspeichersystem](#).

Anforderungssyntax

```
{
  "AccessKey": "string",
  "AgentArns": [ "string" ],
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "LocationArn": "string",
  "SecretKey": "string",
  "ServerCertificate": blob,
  "ServerHostname": "string",
  "ServerPort": number,
  "ServerProtocol": "string",
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[AccessKey](#)

Gibt den Zugriffsschlüssel (z. B. einen Benutzernamen) an, wenn Anmeldeinformationen für die Authentifizierung beim Objektspeicher-Server erforderlich sind.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Höchstlänge = 200 Zeichen.

Pattern: `^.*$`

Erforderlich: Nein

[AgentArns](#)

(Optional) Gibt die Amazon-Ressourcennamen (ARNs) der DataSync Agenten an, die eine Verbindung zu Ihrem Objektspeichersystem herstellen können. Wenn Sie eine cloudübergreifende Übertragung ohne Agenten einrichten, müssen Sie für diesen Parameter keinen Wert angeben.

Note

Sie können keine Agenten zu einem Speicherort hinzufügen oder daraus entfernen, nachdem Sie ihn ursprünglich erstellt haben.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

[CmkSecretConfig](#)

Gibt Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis an, z. B. ein Authentifizierungstoken oder einen Satz von Anmeldeinformationen, das für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet wird, und für einen vom AWS KMS key Kunden verwalteten Schlüssel.

Typ: [CmkSecretConfig](#) Objekt

Erforderlich: Nein

CustomSecretConfig

Gibt Konfigurationsinformationen für ein vom Kunden verwaltetes Geheimnis an, z. B. ein Authentifizierungstoken oder einen Satz von Anmeldeinformationen, das für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet wird, und für ein vom Kunden verwaltetes Geheimnis. AWS KMS key

Typ: [CustomSecretConfig](#) Objekt

Erforderlich: Nein

LocationArn

Gibt den ARN des Objektspeichersystems an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

SecretKey

Gibt den geheimen Schlüssel (z. B. ein Passwort) an, wenn Anmeldeinformationen für die Authentifizierung beim Objektspeicher-Server erforderlich sind.

Note

Wenn Sie mithilfe von `CmkSecretConfig` oder ein Geheimnis angeben `SecretKey`, aber keine geheimen Konfigurationsdetails angeben `CustomSecretConfig`, DataSync speichert das Token unter Verwendung des Secrets Manager Manager-Geheimnisses Ihres AWS Kontos.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Höchstlänge = 200 Zeichen.

Pattern: `^.*$`

Erforderlich: Nein

ServerCertificate

Gibt eine Zertifikatskette für DataSync die Authentifizierung bei Ihrem Objektspeichersystem an, falls das System eine private oder selbstsignierte Zertifizierungsstelle (CA) verwendet. Sie müssen eine einzelne .pem Datei mit einer vollständigen Zertifikatskette angeben (z. B. `file:///home/user/.ssh/object_storage_certificates.pem`).

Die Zertifikatskette könnte Folgendes beinhalten:

- Das Zertifikat des Objektspeichersystems
- Alle Zwischenzertifikate (falls vorhanden)
- Das Stammzertifikat der signierenden Zertifizierungsstelle

Sie können Ihre Zertifikate zu einer .pem Datei zusammenfügen (die vor der Base64-Kodierung bis zu 32768 Byte groß sein kann). Mit dem folgenden `cat` Beispielbefehl wird eine `object_storage_certificates.pem` Datei erstellt, die drei Zertifikate enthält:

```
cat object_server_certificate.pem intermediate_certificate.pem
ca_root_certificate.pem > object_storage_certificates.pem
```

Um diesen Parameter zu verwenden, konfigurieren Sie `ServerProtocol` auf `HTTPS`.

Die Aktualisierung dieses Parameters beeinträchtigt nicht die Aufgaben, die Sie gerade ausführen.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 32768.

Erforderlich: Nein

ServerHostname

Gibt den Domännennamen oder die IP-Adresse (IPv4 oder IPv6) des Objektspeicherservers an, mit dem Ihr DataSync Agent eine Verbindung herstellt.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^(( [a-zA-Z0-9\-\ ]*[a-zA-Z0-9] )\.)*([A-Za-z0-9\-\ :]*[A-Za-z0-9])$`

Erforderlich: Nein

ServerPort

Gibt den Port an, an dem Ihr Objektspeicher-Server eingehenden Netzwerkverkehr annimmt (z. B. Port 443).

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Der Höchstwert ist 65536.

Erforderlich: Nein

ServerProtocol

Gibt das Protokoll an, das Ihr Objektspeicher-Server für die Kommunikation verwendet.

Typ: Zeichenfolge

Zulässige Werte: HTTPS | HTTP

Erforderlich: Nein

Subdirectory

Gibt das Objekt-Präfix für Ihren Objektspeicher-Server an. Wenn es sich um einen Quellspeicherort handelt, werden DataSync nur Objekte mit diesem Präfix kopiert. Wenn es sich um einen Zielort handelt, werden alle Objekte mit diesem Präfix DataSync geschrieben.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationS3

Ändert die folgenden Konfigurationsparameter des Amazon S3 S3-Übertragungsorts, den Sie mit AWS DataSync verwenden.

Important

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Themen gelesen haben:

- [Überlegungen zur Speicherkategorie bei Amazon S3 S3-Standorten](#)
- [Bewertung der Kosten für S3-Anfragen bei der Verwendung DataSync](#)

Anforderungssyntax

```
{
  "LocationArn": "string",
  "S3Config": {
    "BucketAccessRoleArn": "string"
  },
  "S3StorageClass": "string",
  "Subdirectory": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[LocationArn](#)

Gibt den Amazon-Ressourcennamen (ARN) des Amazon S3-Übertragungsorts an, den Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Ja

S3Config

Gibt den Amazon-Ressourcennamen (ARN) der AWS Identity and Access Management (IAM) - Rolle an, die für den Zugriff auf Ihren S3-Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [DataSync Zugriff auf S3-Buckets bereitstellen](#).

Typ: [S3Config](#) Objekt

Erforderlich: Nein

S3StorageClass

Gibt die Speicherklasse an, die Ihre Objekte verwenden sollen, wenn Amazon S3 ein Übertragungsziel ist.

Für Buckets in ist AWS-Regionen die Speicherklasse standardmäßig auf eingestellt. STANDARD
Bei aktivierten Buckets ist AWS Outposts die Speicherklasse standardmäßig auf. OUTPOSTS

Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#).

Typ: Zeichenfolge

Zulässige Werte: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING |
GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Erforderlich: Nein

Subdirectory

Gibt ein Präfix im S3-Bucket an, das DataSync Lese- oder Schreibvorgänge vornimmt (je nachdem, ob es sich bei dem Bucket um einen Quell- oder Zielspeicherort handelt).

Note

DataSync kann keine Objekte mit einem Präfix übertragen, das mit einem Schrägstrich (/) beginnt oder /. . / Muster einschließt//. /. / Beispiel:

- /photos
- photos//2006/January
- photos/. /2006/February

- photos/./2006/March

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateLocationSmb

Ändert die folgenden Konfigurationsparameter des SMB-Übertragungsorts (Server Message Block), den Sie mit verwenden. AWS DataSync

Weitere Informationen finden Sie unter [Konfiguration von DataSync Übertragungen mit einem SMB-Dateiserver](#).

Anforderungssyntax

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "DnsIpAddresses": [ "string" ],
  "Domain": "string",
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "LocationArn": "string",
  "MountOptions": {
    "Version": "string"
  },
  "Password": "string",
  "ServerHostname": "string",
  "Subdirectory": "string",
  "User": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AgentArns

Gibt den DataSync Agenten (oder die Agenten) an, der eine Verbindung zu Ihrem SMB-Dateiserver herstellen kann. Sie geben einen Agenten anhand seines Amazon-Ressourcennamens (ARN) an.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Artikeln.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

AuthenticationType

Gibt das Authentifizierungsprotokoll an, das für die Verbindung mit Ihrem SMB-Dateiserver DataSync verwendet wird. DataSync unterstützt NTLM (Standard) und KERBEROS Authentifizierung.

Weitere Informationen finden Sie unter [Bereitstellen des DataSync Zugriffs auf SMB-Dateiserver](#).

Typ: Zeichenfolge

Zulässige Werte: NTLM | KERBEROS

Erforderlich: Nein

CmkSecretConfig

Gibt Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis an, z. B. ein Password KerberosKeytab oder eine Gruppe von Anmeldeinformationen, die für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet werden, und für einen vom Kunden verwalteten Schlüssel. AWS KMS key

Typ: [CmkSecretConfig](#) Objekt

Erforderlich: Nein

CustomSecretConfig

Gibt Konfigurationsinformationen für einen vom Kunden verwalteten geheimen Schlüssel an, z. B. einen Password KerberosKeytab oder einen Satz von Anmeldeinformationen, die für den

Zugriff auf einen bestimmten Übertragungsort DataSync verwendet werden, und für einen vom Kunden verwalteten Schlüssel. AWS KMS key

Typ: [CustomSecretConfig](#) Objekt

Erforderlich: Nein

[DnsIpAddresses](#)

Gibt die IP-Adressen (IPv4 oder IPv6) für die DNS-Server an, zu denen Ihr SMB-Dateiserver gehört. Dieser Parameter gilt nur, wenn er auf KERBEROS gesetzt `AuthenticationType` ist.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen SMB-Dateiserver hergestellt wird.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Maximale Anzahl von 2 Elementen.

Längenbeschränkungen: Minimale Länge beträgt 7 Zeichen. Die maximale Länge beträgt 39.

Pattern: `\A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\. (25[0-5]|2[0-4]\d|[0-1]?\d?\d))){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}: [0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(: [0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(: [0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(: [0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(: [0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((: [0-9a-fA-F]{1,4}){1,6}))\z`

Erforderlich: Nein

[Domain](#)

Gibt den Windows-Domain-Namen an, zu dem SMB-Dateiserver gehört. Dieser Parameter gilt nur, wenn er auf gesetzt `AuthenticationType` istNTLM.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zum richtigen Dateiserver hergestellt wird.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]){0,252}$`

Erforderlich: Nein

[KerberosKeytab](#)

Gibt Ihre Kerberos-Schlüsseltabellendatei (Keytab) an, die Zuordnungen zwischen Ihrem Kerberos-Prinzipal und den Verschlüsselungsschlüsseln enthält.

Um Fehler bei der Ausführung von Aufgaben zu vermeiden, stellen Sie sicher, dass der Kerberos-Prinzipal, den Sie zum Erstellen der Keytab-Datei verwenden, genau dem entspricht, wofür Sie es angegeben haben. `KerberosPrincipal`

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 65536.

Erforderlich: Nein

[KerberosKrb5Conf](#)

Gibt eine Kerberos-Konfigurationsdatei (`krb5.conf`) an, die Ihre Kerberos-Realm-Konfiguration definiert.

Die Datei muss Base64-codiert sein. Wenn Sie das verwenden AWS CLI, ist die Kodierung für Sie erledigt.

Typ: Base64-kodiertes Binärdatenobjekt

Längenbeschränkungen: Die maximale Länge beträgt 131072.

Erforderlich: Nein

[KerberosPrincipal](#)

Gibt einen Kerberos-Principal an. Dabei handelt es sich um eine Identität in Ihrem Kerberos-Bereich, die berechtigt ist, auf die Dateien, Ordner und Dateimetadaten auf Ihrem SMB-Dateiserver zuzugreifen.

Ein Kerberos-Prinzipal könnte wie folgt aussehen. `HOST/kerberosuser@MYDOMAIN.ORG`

Bei Prinzipalnamen wird Groß- und Kleinschreibung beachtet. Ihre DataSync Aufgabenausführung schlägt fehl, wenn der Prinzipal, den Sie für diesen Parameter angeben, nicht exakt dem Prinzipal entspricht, den Sie zum Erstellen der Keytab-Datei verwenden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^.+`

Erforderlich: Nein

LocationArn

Gibt den ARN des SMB-Standorts an, den Sie aktualisieren möchten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}`

Erforderlich: Ja

MountOptions

Gibt die Version des SMB-Protokolls (Server Message Block) an, das für den Zugriff auf einen SMB-Dateiserver AWS DataSync verwendet wird.

Typ: [SmbMountOptions](#) Objekt

Erforderlich: Nein

Password

Gibt das Kennwort des Benutzers an, der Ihren SMB-Dateiserver bereitstellen kann und über Zugriffsrechte auf die Dateien und Ordner verfügt, die an Ihrer Übertragung beteiligt sind. Dieser Parameter gilt nur, wenn er auf NTLM gesetzt AuthenticationType ist.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^.{0,104}`

Erforderlich: Nein

ServerHostname

Gibt den Domännennamen oder die IP-Adresse (IPv4 oder IPv6) des SMB-Dateiservers an, mit dem Ihr DataSync Agent eine Verbindung herstellt.

Note

Wenn Sie die Kerberos-Authentifizierung verwenden, müssen Sie einen Domännennamen angeben.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge von 255.

Pattern: `^(( [a-zA-Z0-9\ - ]*[a-zA-Z0-9] )\ . )*( [A-Za-z0-9\ - : ]*[A-Za-z0-9] )$`

Erforderlich: Nein

Subdirectory

Gibt den Namen der von Ihrem SMB-Dateiserver exportierten Freigabe an, auf der Daten gelesen oder geschrieben DataSync werden. Sie können ein Unterverzeichnis in den Freigabepfad aufnehmen (z. B. /path/to/subdirectory). Stellen Sie sicher, dass andere SMB-Clients in Ihrem Netzwerk diesen Pfad ebenfalls bereitstellen können.

Um alle Daten im angegebenen Unterverzeichnis zu kopieren, DataSync müssen Sie in der Lage sein, die SMB-Freigabe zu mounten und auf alle zugehörigen Daten zuzugreifen. Weitere Informationen finden Sie unter [DataSync Zugriff auf SMB-Dateiserver bereitstellen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\ -\ +\ .\/\ (\)\ \ $\p{Zs} ]+$`

Erforderlich: Nein

User

Gibt den Benutzernamen an, der Ihren SMB-Dateiserver mounten kann und der Zugriff auf die Dateien und Ordner hat, die an Ihrer Übertragung beteiligt sind. Dieser Parameter gilt nur, wenn er auf NTLM gesetzt AuthenticationType ist.

Informationen zur Auswahl eines Benutzers mit der richtigen Zugriffsebene für Ihre Übertragung finden Sie unter [DataSync Zugriff auf SMB-Dateiserver bereitstellen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E]{1,104}$`

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateTask

Aktualisiert die Konfiguration einer Aufgabe, die definiert, wo und wie Ihre Daten AWS DataSync übertragen werden.

Anforderungssyntax

```
{
  "CloudWatchLogGroupArn": "string",
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
      }
    }
  },
  "Name": "string",
  "Options": {
    "Atime": "string",
    "BytesPerSecond": number,
    "Gid": "string",
    "LogLevel": "string",
    "Mtime": "string",
    "ObjectTags": "string",
    "OverwriteMode": "string",
    "PosixPermissions": "string",
```

```

    "PreserveDeletedFiles": "string",
    "PreserveDevices": "string",
    "SecurityDescriptorCopyFlags": "string",
    "TaskQueueing": "string",
    "TransferMode": "string",
    "Uid": "string",
    "VerifyMode": "string"
  },
  "Schedule": {
    "ScheduleExpression": "string",
    "Status": "string"
  },
  "TaskArn": "string",
  "TaskReportConfig": {
    "Destination": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "S3BucketArn": "string",
        "Subdirectory": "string"
      }
    },
    "ObjectVersionIds": "string",
    "OutputType": "string",
    "Overrides": {
      "Deleted": {
        "ReportLevel": "string"
      },
      "Skipped": {
        "ReportLevel": "string"
      },
      "Transferred": {
        "ReportLevel": "string"
      },
      "Verified": {
        "ReportLevel": "string"
      }
    },
    "ReportLevel": "string"
  }
}

```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[CloudWatchLogGroupArn](#)

Gibt den Amazon-Ressourcennamen (ARN) einer CloudWatch Amazon-Protokollgruppe zur Überwachung Ihrer Aufgabe an.

Für Aufgaben im erweiterten Modus müssen Sie den Namen Ihrer Protokollgruppe verwenden/ aws/datasync. Beispiel:

```
arn:aws:logs:us-east-1:111222333444:log-group:/aws/datasync:*
```

Weitere Informationen finden Sie unter [Überwachen von Datenübertragungen mit CloudWatch Protokollen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 562.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)*$`

Erforderlich: Nein

[Excludes](#)

Gibt Ausschlussfilter an, die die Dateien, Objekte und Ordner in Ihrem Quellverzeichnis definieren, die Sie nicht übertragen DataSync möchten. Weitere Informationen und Beispiele finden Sie unter [Mithilfe von Filtern angeben, welche DataSync Übertragungen übertragen werden](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

Erforderlich: Nein

Includes

Gibt an, dass Include-Filter die Dateien, Objekte und Ordner an Ihrem Quellspeicherort definieren, die Sie übertragen DataSync möchten. Weitere Informationen und Beispiele finden Sie unter [Mithilfe von Filtern angeben, welche DataSync Übertragungen übertragen werden](#).

Typ: Array von [FilterRule](#)-Objekten

Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 1 Element.

Erforderlich: Nein

ManifestConfig

Konfiguriert ein Manifest, bei dem es sich um eine Liste von Dateien oder Objekten handelt, die Sie übertragen DataSync möchten. Weitere Informationen und Konfigurationsbeispiele finden Sie unter [Angabe der DataSync Übertragungen mithilfe eines Manifests](#).

Wenn Sie diesen Parameter verwenden, muss Ihre Anruferidentität (die IAM-Rolle, die Sie DataSync mit verwenden) über die `iam:PassRole` entsprechende Berechtigung verfügen. Die [AWSDataSyncFullAccess](#) Richtlinie beinhaltet diese Berechtigung.

Um eine Manifestkonfiguration zu entfernen, geben Sie diesen Parameter als leer an.

Typ: [ManifestConfig](#) Objekt

Erforderlich: Nein

Name

Gibt den Namen Ihrer Aufgabe an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\+=. _:@/-]+$`

Erforderlich: Nein

Options

Gibt an, wie Ihre Übertragungsaufgabe konfiguriert ist. Zu diesen Optionen gehört, DataSync wie mit Dateien, Objekten und den zugehörigen Metadaten während der Übertragung umgegangen

wird. Sie können unter anderem auch angeben, wie die Datenintegrität überprüft werden soll, Bandbreitenlimits für Ihre Aufgabe festlegen.

Jede Option hat einen Standardwert. Sofern Sie dies nicht möchten, müssen Sie vor dem Aufruf keine Option konfigurieren [StartTaskExecution](#).

Sie können Ihre Aufgabenoptionen auch für jede Aufgabenausführung überschreiben. Möglicherweise möchten Sie die `LogLevel` für eine einzelne Ausführung anpassen.

Typ: [Options](#) Objekt

Erforderlich: Nein

[Schedule](#)

Gibt einen Zeitplan an, wann Ihre Aufgabe ausgeführt werden soll. Weitere Informationen finden Sie unter [Aufgabenplanung](#).

Typ: [TaskSchedule](#) Objekt

Erforderlich: Nein

[TaskArn](#)

Gibt den ARN der Aufgabe an, die Sie aktualisieren möchten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erforderlich: Ja

[TaskReportConfig](#)

Gibt an, wie Sie einen Aufgabenbericht konfigurieren möchten, der detaillierte Informationen zu Ihrer DataSync Übertragung enthält. Weitere Informationen finden Sie unter [Überwachen Ihrer DataSync Übertragungen mit Aufgabenberichten](#).

Wenn Sie diesen Parameter verwenden, muss Ihre Anruferidentität (die IAM-Rolle, die Sie DataSync mit verwenden) über die `iam:PassRole` entsprechende Berechtigung verfügen. Die [AWSDataSyncFullAccess](#) Richtlinie beinhaltet diese Berechtigung.

Um eine Task-Berichtskonfiguration zu entfernen, geben Sie diesen Parameter als leer an.

Typ: [TaskReportConfig](#) Objekt

Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Dienst ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)

- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

UpdateTaskExecution

Aktualisiert die Konfiguration einer laufenden AWS DataSync Aufgabenausführung.

Note

Derzeit können Sie nur Änderungen vornehmen `Option`, indem die Bandbreite für die Ausführung einer laufenden oder in der Warteschlange befindlichen Aufgabe gedrosselt wird. `UpdateTaskExecution` [BytesPerSecond](#)

Anforderungssyntax

```
{
  "Options": {
    "Atime": "string",
    "BytesPerSecond": number,
    "Gid": "string",
    "LogLevel": "string",
    "Mtime": "string",
    "ObjectTags": "string",
    "OverwriteMode": "string",
    "PosixPermissions": "string",
    "PreserveDeletedFiles": "string",
    "PreserveDevices": "string",
    "SecurityDescriptorCopyFlags": "string",
    "TaskQueueing": "string",
    "TransferMode": "string",
    "Uid": "string",
    "VerifyMode": "string"
  },
  "TaskExecutionArn": "string"
}
```

Anforderungsparameter

Informationen zu den Parametern, die alle Aktionen gemeinsam haben, finden Sie unter [Allgemeine Parameter](#).

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

[Options](#)

Gibt an, wie Ihre Übertragungsaufgabe konfiguriert ist. Zu diesen Optionen gehört, DataSync wie mit Dateien, Objekten und den zugehörigen Metadaten während der Übertragung umgegangen wird. Sie können unter anderem auch angeben, wie die Datenintegrität überprüft werden soll, Bandbreitenlimits für Ihre Aufgabe festlegen.

Jede Option hat einen Standardwert. Sofern Sie dies nicht möchten, müssen Sie vor dem Anruf keine Option konfigurieren [StartTaskExecution](#).

Sie können Ihre Aufgabenoptionen auch für jede Aufgabenausführung überschreiben. Möglicherweise möchten Sie die `LogLevel` für eine einzelne Ausführung anpassen.

Typ: [Options](#) Objekt

Erforderlich: Ja

[TaskExecutionArn](#)

Gibt den Amazon-Ressourcennamen (ARN) der Aufgabenausführung an, die Sie aktualisieren.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter [Häufige Fehler](#).

InternalException

Diese Ausnahme wird ausgelöst, wenn im AWS DataSync Service ein Fehler auftritt.

HTTP Status Code: 500

InvalidRequestException

Diese Ausnahme wird ausgelöst, wenn der Client eine falsch formatierte Anfrage sendet.

HTTP-Statuscode: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS Befehlszeilenschnittstelle V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK für JavaScript V3](#)
- [AWS SDK für Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK für Python](#)
- [AWS SDK for Ruby V3](#)

Datentypen

Die folgenden Datentypen werden unterstützt:

- [AgentListEntry](#)
- [AzureBlobSasConfiguration](#)
- [CmkSecretConfig](#)
- [CustomSecretConfig](#)

- [Ec2Config](#)
- [FilterRule](#)
- [FsxProtocol](#)
- [FsxProtocolNfs](#)
- [FsxProtocolSmb](#)
- [FsxUpdateProtocol](#)
- [FsxUpdateProtocolSmb](#)
- [HdfsNameNode](#)
- [LocationFilter](#)
- [LocationListEntry](#)
- [ManagedSecretConfig](#)
- [ManifestConfig](#)
- [NfsMountOptions](#)
- [OnPremConfig](#)
- [Options](#)
- [Platform](#)
- [PrivateLinkConfig](#)
- [QopConfiguration](#)
- [ReportDestination](#)
- [ReportDestinationS3](#)
- [ReportOverride](#)
- [ReportOverrides](#)
- [ReportResult](#)
- [S3Config](#)
- [S3ManifestConfig](#)
- [SmbMountOptions](#)
- [SourceManifestConfig](#)
- [TagListEntry](#)
- [TaskExecutionFilesFailedDetail](#)
- [TaskExecutionFilesListedDetail](#)

- [TaskExecutionFoldersFailedDetail](#)
- [TaskExecutionFoldersListedDetail](#)
- [TaskExecutionListEntry](#)
- [TaskExecutionResultDetail](#)
- [TaskFilter](#)
- [TaskListEntry](#)
- [TaskReportConfig](#)
- [TaskSchedule](#)
- [TaskScheduleDetails](#)

AgentListEntry

Stellt einen einzelnen Eintrag in einer Liste (oder einem Array) von AWS DataSync Agenten dar, wenn Sie den [ListAgents](#) Vorgang aufrufen.

Inhalt

AgentArn

Der Amazon-Ressourcenname (ARN) eines DataSync Agenten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Nein

Name

Der Name eines Agenten.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Erforderlich: Nein

Plattform

Die plattformbezogenen Details über den Agenten, wie z. B. die Versionsnummer.

Typ: [Platform](#) Objekt

Erforderlich: Nein

Status

Der Status eines Agenten.

- Wenn der Status lautet `ONLINE`, ist der Agent ordnungsgemäß konfiguriert und einsatzbereit.

- Wenn der Status lautet OFFLINE, hat der Agent seit mindestens fünf DataSync Minuten keinen Kontakt mehr zu Ihnen aufgenommen. Dies kann verschiedene Gründe haben. Weitere Informationen finden Sie unter [Was mache ich, wenn mein Agent offline ist?](#)

Typ: Zeichenfolge

Zulässige Werte: ONLINE | OFFLINE

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AzureBlobSasConfiguration

Die SAS-Konfiguration (Shared Access Signature), die AWS DataSync den Zugriff auf Ihren Microsoft Azure Blob Storage ermöglicht.

Weitere Informationen finden Sie unter [SAS-Token](#) für den Zugriff auf Ihren Azure Blob Storage.

Inhalt

Token

Gibt ein SAS-Token an, das Berechtigungen für den Zugriff auf Ihren Azure Blob Storage bereitstellt.

Das Token ist Teil der SAS-URI-Zeichenfolge, die nach dem Speicherressourcen-URI und einem Fragezeichen steht. Ein Token sieht ungefähr so aus:

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&s%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Pattern: `^.+`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CmkSecretConfig

Gibt Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis an, z. B. ein Authentifizierungstoken, einen geheimen Schlüssel, ein Passwort oder eine Kerberos-Keytab, die für den Zugriff auf einen bestimmten Speicherort DataSync verwendet wird, mit einem vom Kunden verwalteten AWS KMS key

Note

Sie können entweder `CmkSecretConfig` oder verwenden, um Anmeldeinformationen `CustomSecretConfig` für eine Anfrage bereitzustellen. `CreateLocation` Geben Sie nicht beide Parameter für dieselbe Anfrage an.

Inhalt

KmsKeyArn

Gibt den ARN für das vom Kunden verwaltete Objekt an AWS KMS key , das zur Verschlüsselung des gespeicherten DataSync -verwalteten Geheimnisses DataSync verwendet wird. `SecretArn` DataSync stellt diesen Schlüssel bereit für. AWS Secrets Manager

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):kms:[a-z\\-0-9]+:[0-9]{12}:key/.*)$`

Erforderlich: Nein

SecretArn

Gibt den ARN für das DataSync -managed AWS Secrets Manager secret an, das für den Zugriff auf einen bestimmten Speicherort verwendet wird. Diese Eigenschaft wird von generiert DataSync und ist schreibgeschützt. DataSync verschlüsselt dieses Geheimnis mit dem KMS-Schlüssel, den Sie angeben. `KmsKeyArn`

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):secretsmanager:[a-z\-\0-9]+:[0-9]{12}:secret:.*|)$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CustomSecretConfig

Gibt Konfigurationsinformationen für ein vom Kunden verwaltetes Secrets Manager-Geheimnis an, bei dem Anmeldeinformationen für einen Speicherort in Secrets Manager als Klartext (für Authentifizierungstoken, geheimen Schlüssel oder Passwort) oder als Binärdatei (für Kerberos-Keytab) gespeichert werden. Diese Konfiguration umfasst den geheimen ARN und den ARN für eine IAM-Rolle, die Zugriff auf den geheimen Schlüssel ermöglicht.

Note

Sie können entweder `CmkSecretConfig` oder `verwendenCustomSecretConfig`, um Anmeldeinformationen für eine `CreateLocation` Anfrage bereitzustellen. Geben Sie nicht beide Parameter für dieselbe Anfrage an.

Inhalt

SecretAccessRoleArn

Gibt den ARN für die AWS Identity and Access Management Rolle an, die für den Zugriff auf das angegebene Geheimnis DataSync verwendet wird `SecretArn`.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam:[0-9]{12}:role/[a-zA-Z0-9+_,.@-]+)|)$`

Erforderlich: Nein

SecretArn

Gibt den ARN für ein AWS Secrets Manager Geheimnis an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):secretsmanager:[a-z\0-9]+:[0-9]{12}:secret:.*)$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Ec2Config

Das Subnetz und die Sicherheitsgruppen, die für die Verbindung zu einem der [Mount-Ziele](#) Ihres Amazon EFS-Dateisystems AWS DataSync verwendet werden.

Inhalt

SecurityGroupArns

Gibt die Amazon-Ressourcennamen (ARNs) der Sicherheitsgruppen an, die dem Mount-Ziel eines Amazon EFS-Dateisystems zugeordnet sind.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erforderlich: Ja

SubnetArn

Gibt den ARN eines Subnetzes an, in dem die [Netzwerkschnittstellen](#) für die Verwaltung des Datenverkehrs während Ihrer Übertragung DataSync erstellt werden.

Befinden muss sich das Subnetz:

- In derselben Virtual Private Cloud (VPC) wie das Amazon-EFS-Dateisystem.
- In derselben Availability Zone wie mindestens ein Bereitstellungsziel für das Amazon-EFS-Dateisystem.

Note

Sie müssen kein Subnetz angeben, das ein Bereitstellungsziel für das Dateisystem enthält.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\\-0-9]*:[0-9]{12}:subnet/subnet-[a-f0-9]+$`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FilterRule

Gibt an, welche Dateien, Ordner und Objekte beim Übertragen von Dateien von der Quelle zum Ziel eingeschlossen oder ausgeschlossen werden sollen.

Inhalt

FilterType

Der Typ der anzuwendenden Filterregel. AWS DataSync unterstützt nur den Regeltyp `SIMPLE_PATTERN`.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^[A-Z0-9_]+$`

Zulässige Werte: `SIMPLE_PATTERN`

Erforderlich: Nein

Value

Eine einzelne Filterzeichenfolge, die aus den einzubeziehenden oder auszuschließenden Mustern besteht. Die Muster werden durch „|“ (also eine Pipe) begrenzt, zum Beispiel: `/folder1|/folder2`

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 102400.

Pattern: `^[^\x00]+$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FsxProtocol

Gibt das Datenübertragungsprotokoll an, das für den Zugriff auf Ihr FSx Amazon-Dateisystem AWS DataSync verwendet wird.

Inhalt

NFS

Gibt die NFS-Protokollkonfiguration (Network File System) an, die für den Zugriff auf Ihr OpenZFS-Dateisystem oder FSx FSx für die virtuelle Speichermaschine (SVM) des ONTAP-Dateisystems DataSync verwendet wird.

Typ: [FsxProtocolNfs](#) Objekt

Erforderlich: Nein

SMB

Gibt die SMB-Protokollkonfiguration (Server Message Block) an, die FSx für den Zugriff auf die SVM Ihres ONTAP-Dateisystems DataSync verwendet wird.

Typ: [FsxProtocolSmb](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FsxProtocolNfs

Gibt die NFS-Protokollkonfiguration (Network File System) an, die für den Zugriff auf Ihr OpenZFS-Dateisystem oder FSx FSx für die virtuelle Speichermaschine (SVM) des ONTAP-Dateisystems DataSync verwendet wird.

Inhalt

MountOptions

Gibt an, wie mithilfe des DataSync NFS-Protokolls auf einen Speicherort zugegriffen werden kann.

Typ: [NfsMountOptions](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FsxProtocolSmb

Gibt die SMB-Protokollkonfiguration (Server Message Block) an, die für den Zugriff auf die virtuelle Speichermaschine (SVM) Ihres Amazon FSx for NetApp ONTAP-Dateisystems AWS DataSync verwendet wird. Weitere Informationen finden Sie unter [Bereitstellen des DataSync Zugriffs auf FSx ONTAP-Dateisysteme](#).

Inhalt

Password

Gibt das Passwort eines Benutzers an, der berechtigt ist, auf Ihre SVM zuzugreifen.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^\.{0,104}$`

Erforderlich: Ja

User

Gibt einen Benutzer an, der die Dateien, Ordner und Metadaten in Ihrer SVM bereitstellen und darauf zugreifen kann.

Informationen zur Auswahl eines Benutzers mit der richtigen Zugriffsebene für Ihre Übertragung finden Sie unter [Verwenden des SMB-Protokolls](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E]{1,104}$`

Erforderlich: Ja

Domain

Gibt den Namen der Windows-Domäne an, zu der Ihre virtuelle Speichermaschine (SVM) gehört.

Wenn Sie mehrere Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieser Einstellung sichergestellt, dass die DataSync Verbindung zur richtigen SVM hergestellt wird.

Wenn Sie mehrere Active Directory-Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass die DataSync Verbindung zur richtigen SVM hergestellt wird.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Erforderlich: Nein

MountOptions

Gibt die Version des SMB-Protokolls (Server Message Block) an, das für den Zugriff auf einen SMB-Dateiserver AWS DataSync verwendet wird.

Typ: [SmbMountOptions](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FsxUpdateProtocol

Gibt das Datenübertragungsprotokoll an, das für den Zugriff auf Ihr FSx Amazon-Dateisystem AWS DataSync verwendet wird.

Note

Sie können die NFS-Protokollkonfiguration (Network File System) FSx für ONTAP-Standorte nicht aktualisieren. DataSync unterstützt derzeit nur NFS Version 3 mit diesem Speicherortyp.

Inhalt

NFS

Gibt die NFS-Protokollkonfiguration (Network File System) an, die für den Zugriff auf Ihr OpenZFS-Dateisystem oder FSx FSx für die virtuelle Speichermaschine (SVM) des ONTAP-Dateisystems DataSync verwendet wird.

Typ: [FsxProtocolNfs](#) Objekt

Erforderlich: Nein

SMB

Gibt die SMB-Protokollkonfiguration (Server Message Block) an, die FSx für den Zugriff auf die DataSync virtuelle Speichermaschine (SVM) Ihres ONTAP-Dateisystems verwendet wird.

Typ: [FsxUpdateProtocolSmb](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FsxUpdateProtocolSmb

Gibt die SMB-Protokollkonfiguration (Server Message Block) an, die für den Zugriff auf die virtuelle Speichermaschine (SVM) Ihres Amazon FSx for NetApp ONTAP-Dateisystems AWS DataSync verwendet wird. Weitere Informationen finden Sie unter [Bereitstellen des DataSync Zugriffs auf FSx ONTAP-Dateisysteme](#).

Inhalt

Domain

Gibt den Namen der Windows-Domäne an, zu der Ihre virtuelle Speichermaschine (SVM) gehört.

Wenn Sie mehrere Active Directory-Domänen in Ihrer Umgebung haben, wird durch die Konfiguration dieses Parameters sichergestellt, dass DataSync eine Verbindung zur richtigen SVM hergestellt wird.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 253.

Pattern: `^([A-Za-z0-9](\.|-+)?[A-Za-z0-9]){0,252})?$`

Erforderlich: Nein

MountOptions

Gibt die Version des SMB-Protokolls (Server Message Block) an, das für den Zugriff auf einen SMB-Dateiserver AWS DataSync verwendet wird.

Typ: [SmbMountOptions](#) Objekt

Erforderlich: Nein

Password

Gibt das Passwort eines Benutzers an, der berechtigt ist, auf Ihre SVM zuzugreifen.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^.{0,104}$`

Erforderlich: Nein

User

Gibt einen Benutzer an, der die Dateien, Ordner und Metadaten in Ihrer SVM bereitstellen und darauf zugreifen kann.

Informationen zur Auswahl eines Benutzers mit der richtigen Zugriffsebene für Ihre Übertragung finden Sie unter [Verwenden des SMB-Protokolls](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 104.

Pattern: `^[^\\x22\\x5B\\x5D\\/\\:;|=, +*?\\x3C\\x3E]{1,104}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

HdfsNameNode

Das NameNode des Hadoop Distributed File System (HDFS). Das NameNode verwaltet den Namespace des Dateisystems. Der NameNode führt Operationen wie das Öffnen, Schließen und Umbenennen von Dateien und Verzeichnissen aus. Das NameNode enthält die Informationen zum Zuordnen von Datenblöcken zu DataNodes

Inhalt

Hostname

Der Hostname des NameNode im HDFS-Cluster. Dieser Wert ist die IP-Adresse oder der Name des Domain Name Service (DNS) von. NameNode Ein lokal installierter Agent verwendet diesen Hostnamen für die Kommunikation mit dem NameNode im Netzwerk.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Pattern: `^(( [a-zA-Z0-9\ -]*[a-zA-Z0-9])\.)*( [A-Za-z0-9\ -]*[A-Za-z0-9])$`

Erforderlich: Ja

Port

Der Port, den der NameNode verwendet, um Client-Anfragen abzuhören.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Der Maximalwert ist 65536.

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

LocationFilter

Grenzen Sie die Liste der zurückgegebenen Ressourcen ein von `ListLocations`. Um beispielsweise alle Ihre Amazon S3 S3-Standorte zu sehen, erstellen Sie einen Filter mit "Name": "LocationType" "Operator": "Equals", und "Values": "S3".

Weitere Informationen finden Sie unter [Ressourcen filtern](#).

Inhalt

Name

Der Name des verwendeten Filters. Jeder API-Aufruf unterstützt eine Liste von Filtern, die für ihn verfügbar sind (z. B. `LocationType` für `ListLocations`).

Typ: Zeichenfolge

Zulässige Werte: `LocationUri` | `LocationType` | `CreationTime`

Erforderlich: Ja

Operator

Der Operator, der zum Vergleichen von Filterwerten verwendet wird (z. B. `Equals` oder `Contains`).

Typ: Zeichenfolge

Zulässige Werte: `Equals` | `NotEquals` | `In` | `LessThanOrEqual` | `LessThan` | `GreaterThanOrEqual` | `GreaterThan` | `Contains` | `NotContains` | `BeginsWith`

Erforderlich: Ja

Values

Die Werte, nach denen Sie filtern möchten. Beispielsweise möchten Sie möglicherweise nur Amazon S3 S3-Standorte anzeigen.

Typ: Zeichenfolgen-Array

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Pattern: `^[0-9a-zA-Z_\ \-\:\*\.\ \\/\?\-]*$`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

LocationListEntry

Stellt einen einzelnen Eintrag in einer Liste von Orten dar. `LocationListEntry` gibt ein Array zurück, das eine Liste von Speicherorten enthält, wenn die [ListLocations](#) Operation aufgerufen wird.

Inhalt

LocationArn

Der Amazon-Ressourcenname (ARN) des Standorts. Für Network File System (NFS) oder Amazon EFS ist der Speicherort der Exportpfad. Für Amazon S3 ist der Speicherort der Präfixpfad, den Sie mounten und als Stammverzeichnis des Speicherorts verwenden möchten.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erforderlich: Nein

LocationUri

Stellt eine Liste URIs eines Standorts dar. `LocationUri` gibt ein Array zurück, das eine Liste von Speicherorten enthält, wenn die [ListLocations](#) Operation aufgerufen wird.

Format: `TYPE://GLOBAL_ID/SUBDIR`.

TYPE bezeichnet den Typ des Standorts (z. B. `nfs` oder `s3`).

GLOBAL_ID ist der global eindeutige Bezeichner der Ressource, die hinter dem Standort steht. Ein Beispiel für EFS ist `us-east-2.fs-abcd1234`. Ein Beispiel für Amazon S3 ist der Bucket-Name, wie `myBucket` z. Ein Beispiel für NFS ist eine gültige IPv6 OR-Adresse IPv4 oder ein Hostname, der DNS-konform ist.

SUBDIR ist ein gültiger Dateisystempfad, der wie bei der *nix-Konvention durch Schrägstriche getrennt wird. Für NFS und Amazon EFS ist dies der Exportpfad zum Mounten des Speicherorts. Für Amazon S3 ist es der Präfixpfad, den Sie bereitstellen und den Sie als Stammverzeichnis des Speicherorts behandeln.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4360.

Pattern: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ManagedSecretConfig

Gibt Konfigurationsinformationen für ein DataSync verwaltetes Geheimnis an, z. B. ein Authentifizierungstoken oder einen Satz von Anmeldeinformationen, die für den Zugriff auf einen bestimmten Übertragungsort DataSync verwendet werden. DataSync verwendet den standardmäßigen AWS verwalteten KMS-Schlüssel, um dieses Geheimnis zu verschlüsseln. AWS Secrets Manager

Inhalt

SecretArn

Gibt den ARN für ein AWS Secrets Manager Geheimnis an.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):secretsmanager:[a-z\-\0-9]+:[0-9]{12}:secret:.*)$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ManifestConfig

Konfiguriert ein Manifest, das eine Liste von Dateien oder Objekten ist, die Sie übertragen AWS DataSync möchten. Weitere Informationen und Konfigurationsbeispiele finden Sie unter [Angabe der DataSync Übertragungen mithilfe eines Manifests](#).

Inhalt

Action

Gibt an, wofür das Manifest DataSync verwendet wird.

Typ: Zeichenfolge

Zulässige Werte: TRANSFER

Erforderlich: Nein

Format

Gibt das Dateiformat Ihres Manifests an. Weitere Informationen finden Sie unter [Manifest erstellen](#).

Typ: Zeichenfolge

Zulässige Werte: CSV

Erforderlich: Nein

Source

Gibt das Manifest an, das Sie verwenden DataSync möchten, und wo es gehostet wird.

Note

Sie müssen diesen Parameter angeben, wenn Sie am oder nach dem 7. Februar 2024 ein neues Manifest konfigurieren.

Andernfalls erhalten Sie den Statuscode 400 und die `ValidationException` Fehlermeldung, dass Ihnen die IAM-Rolle für DataSync den Zugriff auf den S3-Bucket fehlt, in dem Sie Ihr Manifest hosten. Weitere Informationen finden Sie unter [DataSync Zugriff auf Ihr Manifest bereitstellen](#).

Typ: [SourceManifestConfig](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

NfsMountOptions

Gibt an, wie mit dem NFS-Protokoll auf einen Standort zugegriffen werden DataSync kann.

Inhalt

Version

Gibt die NFS-Version an, die Sie beim Mounten Ihrer NFS-Freigabe verwenden möchten DataSync . Wenn der Server die Verwendung der angegebenen Version verweigert, schlägt die Aufgabe fehl.

Sie können die folgenden Optionen angeben:

- **AUTOMATIC**(Standard): DataSync wählt NFS-Version 4.1.
- **NFS3**: Zustandslose Protokollversion, die asynchrone Schreibvorgänge auf dem Server erlaubt.
- **NFSv4_0**: Zustandsbehaftete, Firewall-freundliche Protokollversion, die Delegationen und Pseudo-Dateisysteme unterstützt.
- **NFSv4_1**: Zustandsbehaftete Protokollversion, die Sitzungen, Verzeichnisdelegierungen und parallele Datenverarbeitung unterstützt. Die NFS-Version 4.1 enthält auch alle in Version 4.0 verfügbaren Funktionen.

Note

DataSync unterstützt derzeit nur NFS Version 3 mit Amazon FSx für NetApp ONTAP-Standorte.

Typ: Zeichenfolge

Zulässige Werte: **AUTOMATIC** | **NFS3** | **NFS4_0** | **NFS4_1**

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

OnPremConfig

Die AWS DataSync Agenten, die eine Verbindung zu Ihrem Network File System (NFS) -Dateiserver herstellen können.

Inhalt

AgentArns

Die Amazon-Ressourcennamen (ARNs) der DataSync Agenten, die eine Verbindung zu Ihrem NFS-Dateiserver herstellen können.

Sie können mehr als einen Agenten angeben. Weitere Informationen finden Sie unter [Mehrere DataSync Agenten verwenden](#).

Typ: Zeichenfolgen-Array

Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Maximale Anzahl von 8 Elementen.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Options

Zeigt an, wie Ihre Übertragungsaufgabe konfiguriert ist. Zu diesen Optionen gehört, DataSync wie mit Dateien, Objekten und den zugehörigen Metadaten während der Übertragung umgegangen wird. Sie können unter anderem auch angeben, wie die Datenintegrität überprüft werden soll, Bandbreitenlimits für Ihre Aufgabe festlegen.

Jede Option hat einen Standardwert. Sofern Sie dies nicht möchten, müssen Sie vor dem Anruf keine Option konfigurieren [StartTaskExecution](#).

Sie können Ihre Aufgabenoptionen auch für jede Aufgabenausführung überschreiben. Möglicherweise möchten Sie die `LogLevel` für eine einzelne Ausführung anpassen.

Inhalt

Atime

Gibt an, ob Metadaten beibehalten werden sollen, die angeben, wann eine Datei zuletzt gelesen oder geschrieben wurde.

Note

Das Verhalten von `Atime` ist plattformübergreifend nicht vollständig standardisiert und DataSync kann daher nur nach bestem Wissen und Gewissen durchgeführt werden.

- `BEST_EFFORT(Standard)` — DataSync versucht, das ursprüngliche `Atime` Attribut für alle Quelldateien beizubehalten (d. h. die Version vor den PREPARING Schritten der Aufgabenausführung). Diese Option wird empfohlen.
- `NONE`- Ignoriert. `Atime`

Note

Wenn `Atime` auf `BEST_EFFORT` festgelegt ist, muss `Mtime` auf `PRESERVE` festgelegt werden.

Wenn `Atime` auf `NONE` festgelegt ist, muss `Mtime` auch `NONE` sein.

Typ: Zeichenfolge

Zulässige Werte: NONE | BEST_EFFORT

Erforderlich: Nein

BytesPerSecond

Schränkt die von einer DataSync Aufgabe verwendete Bandbreite ein. Wenn Sie beispielsweise maximal 1 MB verwenden DataSync möchten, setzen Sie diesen Wert auf 1048576 (=1024*1024).

Type: Long

Gültiger Bereich: Mindestwert -1.

Erforderlich: Nein

Gid

Gibt die POSIX-Gruppen-ID (GID) der Eigentümer der Datei an.

- INT_VALUE(Standard) — Behält den ganzzahligen Wert von Benutzer-ID (UID) und GID bei, was empfohlen wird.
- NONE- Ignoriert UID und GID.

Weitere Informationen finden Sie unter [Grundlegendes zum DataSync Umgang mit Datei- und Objektmetadaten](#).

Typ: Zeichenfolge

Zulässige Werte: NONE | INT_VALUE | NAME | BOTH

Erforderlich: Nein

LogLevel

Gibt den Typ der Protokolle an, die in einer Amazon CloudWatch Logs-Protokollgruppe DataSync veröffentlicht werden. Informationen zur Angabe der Protokollgruppe finden Sie unter [CloudWatchLogGroupArn](#).

- BASIC- Veröffentlicht Protokolle, die nur grundlegende Informationen enthalten (z. B. Übertragungsfehler).
- TRANSFER- Veröffentlicht Protokolle für alle Dateien oder Objekte, die Ihre DataSync Aufgabe überträgt, und führt Datenintegritätsprüfungen durch.

- OFF- Es werden keine Protokolle veröffentlicht.

Typ: Zeichenfolge

Zulässige Werte: OFF | BASIC | TRANSFER

Erforderlich: Nein

Mtime

Gibt an, ob Metadaten beibehalten werden sollen, die angeben, wann vor dem PREPARING Schritt Ihrer Aufgabenausführung das letzte Mal in eine Datei geschrieben wurde. Diese Option ist erforderlich, wenn Sie eine Aufgabe mehrmals ausführen müssen.

- PRESERVE(Standard) — Behält das Original beiMtime, was empfohlen wird.
- NONE- IgnoriertMtime.

Note

Wenn Mtime auf PRESERVE festgelegt ist, muss Atime auf BEST_EFFORT festgelegt werden.

Wenn Mtime auf NONE festgelegt ist, muss Atime auch auf NONE festgelegt werden.

Typ: Zeichenfolge

Zulässige Werte: NONE | PRESERVE

Erforderlich: Nein

ObjectTags

Gibt an, ob Sie bei der Übertragung zwischen PRESERVE Objektspeichersystemen Objekt-Tags verwenden möchten DataSync (Standardverhalten). Wenn Sie möchten, dass Ihre DataSync Aufgabe Objekt-Tags ignoriert, geben Sie den NONE Wert an.

Typ: Zeichenfolge

Zulässige Werte: PRESERVE | NONE

Erforderlich: Nein

OverwriteMode

Gibt an, ob Daten am Zielort geändert oder beibehalten werden DataSync sollen.

- ALWAYS(Standard) — DataSync ändert Daten am Zielspeicherort, wenn sich Quelldaten (einschließlich Metadaten) geändert haben.

Wenn Objekte DataSync überschrieben werden, können zusätzliche Gebühren für bestimmte Amazon S3 S3-Speicherklassen anfallen (z. B. für das Abrufen oder vorzeitiges Löschen).

Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Übertragungen](#).

- NEVER- überschreibt DataSync keine Daten am Zielort, selbst wenn sich die Quelldaten geändert haben. Sie können diese Option verwenden, um vor dem Überschreiben von Änderungen zu schützen, die an Dateien oder Objekten im Ziel vorgenommen wurden.

Typ: Zeichenfolge

Zulässige Werte: ALWAYS | NEVER

Erforderlich: Nein

PosixPermissions

Gibt an, welche Benutzer oder Gruppen für einen bestimmten Zweck auf eine Datei zugreifen können, z. B. zum Lesen, Schreiben oder Ausführen der Datei.

Weitere Informationen finden Sie unter [Grundlegendes zum DataSync Umgang mit Datei- und Objektmetadaten](#).

- PRESERVE(Standard) — Behält Berechtigungen im POSIX-Stil bei, was empfohlen wird.
- NONE- Ignoriert Berechtigungen im POSIX-Stil.

Note

DataSync kann bestehende Berechtigungen eines Quellverzeichnis beibehalten.

Typ: Zeichenfolge

Zulässige Werte: NONE | PRESERVE

Erforderlich: Nein

PreserveDeletedFiles

Gibt an, ob Dateien im Zielverzeichnis, die in der Quelle nicht existieren, beibehalten werden sollen. Diese Option kann sich auf Ihre Amazon S3 S3-Speicherkosten auswirken. Wenn Ihre Aufgabe Objekte löscht, fallen für bestimmte Speicherklassen möglicherweise Mindestspeicherdauergebühren an. Ausführliche Informationen finden Sie unter [Überlegungen bei der Arbeit mit Amazon S3 S3-Speicherklassen in DataSync](#).

- PRESERVE(Standard) — Ignoriert solche Zieldateien, was empfohlen wird.
- REMOVE- Löscht Zieldateien, die in der Quelle nicht vorhanden sind.

Note

Wenn Sie diesen Parameter auf `REMOVE` setzen, können Sie nicht `TransferMode` auf `ALL` setzen. Wenn Sie alle Daten übertragen, wird Ihr Zielort DataSync nicht gescannt und Sie wissen nicht, was gelöscht werden soll.

Typ: Zeichenfolge

Zulässige Werte: PRESERVE | REMOVE

Erforderlich: Nein

PreserveDevices

Gibt an, ob die Metadaten von Block- und Zeichengeräten am Quellspeicherort beibehalten und die Dateien mit diesem Gerätenamen und den Metadaten am Ziel neu erstellt werden DataSync sollen. DataSync kopiert nur den Namen und die Metadaten solcher Geräte.

Note

DataSync kann den tatsächlichen Inhalt dieser Geräte nicht kopieren, da sie keine Endgeräte sind und keine end-of-file (EOF-) Markierung zurückgeben.

- NONE(Standard) — Ignoriert spezielle Geräte (empfohlen).
- PRESERVE- Behält die Zeichen- und Blockgeräte-Metadaten bei. Diese Option wird derzeit für Amazon EFS nicht unterstützt.

Typ: Zeichenfolge

Zulässige Werte: NONE | PRESERVE

Erforderlich: Nein

SecurityDescriptorCopyFlags

Gibt an, welche Komponenten der SMB-Sicherheitsbeschreibung von Quell- in Zielobjekte kopiert werden.

Dieser Wert wird nur für Übertragungen zwischen SMB- und FSx Amazon-Dateiserverstandorten oder zwischen zwei Speicherorten FSx für Windows-Dateiserver verwendet. Weitere Informationen finden Sie unter [Grundlegendes zum DataSync Umgang mit Datei- und Objektmetadaten](#).

- OWNER_DACL(Standard) — Kopiert für jedes DataSync kopierte Objekt die folgenden Metadaten:
 - Der Objekteigentümer.
 - Diskretionäre NTFS-Zugriffskontrolllisten (DACLs), die festlegen, ob Zugriff auf ein Objekt gewährt wird.

DataSync kopiert mit dieser Option keine NTFS-Systemzugriffskontrolllisten (SACLs).

- OWNER_DACL_SACL- Kopiert für jedes DataSync kopierte Objekt die folgenden Metadaten:
 - Der Besitzer des Objekts.
 - Diskretionäre NTFS-Zugriffskontrolllisten (DACLs), die festlegen, ob Zugriff auf ein Objekt gewährt wird.
 - SACLs, die von Administratoren verwendet werden, um Zugriffsversuche auf ein geschütztes Objekt zu protokollieren.

Zum Kopieren SACLs müssen dem Windows-Benutzer, der für den Zugriff auf Ihren SMB-Standort DataSync verwendet wird, zusätzliche Berechtigungen erteilt werden. Informationen zur Auswahl eines Benutzers mit den richtigen Berechtigungen finden Sie unter [Erforderliche Berechtigungen für SMB](#), [FSx für Windows File Server](#) oder [FSx für ONTAP](#) (je nach Art des Speicherorts in Ihrer Übertragung).

- NONE- Keine der Komponenten der SMB-Sicherheitsbeschreibung wird kopiert. Zielobjekte gehören dem Benutzer, der für den Zugriff auf den Zielort angegeben wurde. DACLs und SACLs werden auf der Grundlage der Konfiguration des Zielservers festgelegt.

Typ: Zeichenfolge

Zulässige Werte: NONE | OWNER_DACL | OWNER_DACL_SACL

Erforderlich: Nein

TaskQueueing

Gibt an, ob Ihre Übertragungsaufgaben in bestimmten Szenarien, wenn [mehrere Aufgaben ausgeführt](#) werden, in eine Warteschlange gestellt werden sollen. Dies ist ENABLED die Standardeinstellung.

Typ: Zeichenfolge

Zulässige Werte: ENABLED | DISABLED

Erforderlich: Nein

TransferMode

Gibt an, ob nach einer ersten Kopie nur die Daten (einschließlich Metadaten) DataSync übertragen werden, die sich zwischen den Speicherorten unterscheiden, oder ob bei jeder Ausführung der Aufgabe alle Daten übertragen werden. Wenn Sie wiederkehrende Übertragungen planen, möchten Sie möglicherweise nur die Änderungen übertragen, die sich seit der letzten Ausführung der Aufgabe geändert haben.

- CHANGED(Standard) — DataSync Kopiert nach der ersten vollständigen Übertragung nur die Daten und Metadaten, die sich zwischen Quell- und Zielort unterscheiden.
- ALL- DataSync kopiert alles in der Quelle an das Ziel, ohne die Unterschiede zwischen den Speicherorten zu vergleichen.

Typ: Zeichenfolge

Zulässige Werte: CHANGED | ALL

Erforderlich: Nein

Uid

Gibt die POSIX-Benutzer-ID (UID) des Besitzers der Datei an.

- INT_VALUE(Standard) — Behält den ganzzahligen Wert von UID und Gruppen-ID (GID) bei, was empfohlen wird.
- NONE- Ignoriert UID und GID.

Weitere Informationen finden Sie unter [Metadaten](#) kopiert von. DataSync

Typ: Zeichenfolge

Zulässige Werte: NONE | INT_VALUE | NAME | BOTH

Erforderlich: Nein

VerifyMode

Gibt an, ob und wie die Integrität Ihrer Daten am Ende der Übertragung DataSync überprüft wird.

- ONLY_FILES_TRANSFERRED(empfohlen) — DataSync berechnet die Prüfsumme der übertragenen Daten (einschließlich Metadaten) am Quellspeicherort. Am Ende der Übertragung DataSync wird dann diese Prüfsumme mit der Prüfsumme verglichen, die anhand dieser Daten am Ziel berechnet wurde.

 Note

Dies ist die Standardoption für Aufgaben [im erweiterten Modus](#).

Wir empfehlen diese Option bei der Übertragung in die Speicherklassen S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive. Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Standorten](#).

- POINT_IN_TIME_CONSISTENT— DataSync überprüft am Ende der Übertragung die gesamte Quelle und das Ziel, um sicherzustellen, dass beide Standorte vollständig synchronisiert sind.

 Note

Dies ist die Standardoption für [Aufgaben im Basismodus](#) und wird derzeit nicht für Aufgaben im erweiterten Modus unterstützt.

Wenn Sie ein [Manifest](#) verwenden, wird DataSync nur gescannt und verifiziert, was im Manifest aufgeführt ist.

Sie können diese Option nicht verwenden, wenn Sie zu den Speicherklassen S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive übertragen. Weitere Informationen finden Sie unter [Überlegungen zur Speicherklasse bei Amazon S3 S3-Standorten](#).

- NONE- DataSync führt Datenintegritätsprüfungen nur während Ihrer Übertragung durch. Im Gegensatz zu anderen Optionen erfolgt am Ende Ihrer Übertragung keine zusätzliche Überprüfung.

Typ: Zeichenfolge

Zulässige Werte: POINT_IN_TIME_CONSISTENT | ONLY_FILES_TRANSFERRED | NONE

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Plattform

Die plattformbezogenen Details zum AWS DataSync Agenten, z. B. die Versionsnummer.

Inhalt

Version

Die Version des DataSync Agenten.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PrivateLinkConfig

Gibt an, wie Ihr AWS DataSync Agent AWS mithilfe eines [Virtual Private Cloud \(VPC\) - Dienstendpunkts](#) eine Verbindung herstellt. Ein Agent, der einen VPC-Endpunkt verwendet, ist nicht über das öffentliche Internet zugänglich.

Inhalt

PrivateLinkEndpoint

Gibt den VPC-Endpunkt an [AWS PrivateLink](#), zu dem Ihr Agent eine Verbindung herstellt.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 7 Zeichen. Maximale Länge beträgt 15 Zeichen.

Pattern: `\A(25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d)){3}\z`

Erforderlich: Nein

SecurityGroupArns

Gibt die Amazon-Ressourcennamen (ARN) der Sicherheitsgruppe an, die den DataSync Zugriff auf Ihren VPC-Endpunkt ermöglicht. Sie können nur einen ARN angeben.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Feste Anzahl von 1 Element.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erforderlich: Nein

SubnetArns

Gibt den ARN des Subnetzes an, in dem sich Ihr VPC-Endpunkt befindet. Sie können nur einen ARN angeben.

Typ: Zeichenfolgen-Array

Array-Mitglieder: Feste Anzahl von 1 Element.

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\\-0-9]*:[0-9]{12}:subnet/subnet-[a-f0-9]+$`

Erforderlich: Nein

VpcEndpointId

Gibt die ID des VPC-Endpunkts an, mit dem Ihr Agent eine Verbindung herstellt.

Typ: Zeichenfolge

Pattern: `^vpce-[0-9a-f]{17}$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

QopConfiguration

Die Konfiguration der Quality of Protection (QOP, Schutzqualität) legt den Remote Procedure Call (RPC, Remoteprozeduraufruf) und die Datenschutzeinstellungen für die Datenübertragung fest, die auf dem Hadoop Distributed File System (HDFS)-Cluster konfiguriert sind.

Inhalt

DataTransferProtection

Die auf dem HDFS-Cluster konfigurierte Einstellung für den Datenübertragungsschutz. Diese Einstellung entspricht Ihrer `dfs.data.transfer.protection`-Einstellung in der `hdfs-site.xml`-Datei auf Ihrem Hadoop-Cluster.

Typ: Zeichenfolge

Zulässige Werte: DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY

Erforderlich: Nein

RpcProtection

Die auf dem HDFS-Cluster konfigurierte RPC-Schutzeinstellung. Diese Einstellung entspricht der `hadoop.rpc.protection`-Einstellung in der `core-site.xml`-Datei auf Ihrem Hadoop-Cluster.

Typ: Zeichenfolge

Zulässige Werte: DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im Folgenden AWS SDKs:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportDestination

Gibt an, wo Ihr [Aufgabenbericht DataSync](#) hochgeladen wird.

Inhalt

S3

Gibt den Amazon S3 S3-Bucket an, in den Ihr Aufgabenbericht DataSync hochgeladen wird.

Typ: [ReportDestinationS3](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportDestinationS3

Gibt den Amazon S3 S3-Bucket an, in den Ihr [Aufgabenbericht DataSync](#) hochgeladen wird.

Inhalt

BucketAccessRoleArn

Gibt den Amazon-Ressourcennamen (ARN) der IAM-Richtlinie an, die das Hochladen eines Aufgabenberichts in Ihren S3-Bucket ermöglicht DataSync . Weitere Informationen finden Sie unter [Zulassen DataSync , einen Aufgabenbericht in einen Amazon S3 S3-Bucket hochzuladen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Erforderlich: Ja

S3BucketArn

Gibt den ARN des S3-Buckets an, in den Ihr Bericht DataSync hochgeladen wird.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 268.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:[a-z\-\0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3-outposts:[a-z\-\0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

Erforderlich: Ja

Subdirectory

Gibt ein Bucket-Präfix für Ihren Bericht an.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportOverride

Gibt den Detaillierungsgrad für einen bestimmten Aspekt Ihres DataSync [Aufgabenberichts](#) an.

Inhalt

ReportLevel

Gibt an, ob Ihr Aufgabenbericht nur Fehler oder Erfolge und Fehler enthält.

Beispielsweise könnte Ihr Bericht hauptsächlich nur das enthalten, was bei Ihrer Übertragung nicht gut gelaufen ist (ERRORS_ONLY). Gleichzeitig möchten Sie überprüfen, ob Ihr [Aufgabenfilter](#) ordnungsgemäß funktioniert. In diesem Fall können Sie eine Liste der Dateien abrufen, die DataSync erfolgreich übersprungen wurden und ob etwas übertragen wurde, das Sie nicht übertragen haben (SUCCESES_AND_ERRORS).

Typ: Zeichenfolge

Zulässige Werte: ERRORS_ONLY | SUCCESES_AND_ERRORS

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportOverrides

Der Detaillierungsgrad, der in jedem Aspekt Ihres DataSync [Aufgabenberichts](#) enthalten ist.

Inhalt

Deleted

Gibt die Berichtsebene für die Dateien, Objekte und Verzeichnisse an, die DataSync versucht wurden, an Ihrem Zielort zu löschen. Dies gilt nur, wenn Sie [Ihre Aufgabe so konfigurieren](#), dass Daten am Ziel gelöscht werden, die sich nicht in der Quelle befinden.

Typ: [ReportOverride](#) Objekt

Erforderlich: Nein

Skipped

Gibt die Berichtsebene für die Dateien, Objekte und Verzeichnisse an, die während der Übertragung zu überspringen DataSync versucht wurden.

Typ: [ReportOverride](#) Objekt

Erforderlich: Nein

Transferred

Gibt die Berichtsebene für die Dateien, Objekte und Verzeichnisse an, die DataSync versucht haben, zu übertragen.

Typ: [ReportOverride](#) Objekt

Erforderlich: Nein

Verified

Gibt die Berichtsebene für die Dateien, Objekte und Verzeichnisse an, deren Überprüfung am Ende der Übertragung DataSync versucht wurde.

Typ: [ReportOverride](#) Objekt

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReportResult

Gibt an, ob ein vollständiger [Aufgabenbericht](#) für Ihre Übertragung DataSync erstellt wurde.

Inhalt

ErrorCode

Gibt den Code an, der mit dem Fehler verknüpft ist, falls kein vollständiger Bericht erstellt werden DataSync kann.

Typ: Zeichenfolge

Erforderlich: Nein

ErrorDetail

Enthält Einzelheiten zu Problemen beim Erstellen eines Berichts.

Typ: Zeichenfolge

Erforderlich: Nein

Status

Gibt an, ob noch an Ihrem Bericht gearbeitet DataSync wird, ob ein Bericht erstellt wurde oder ob kein vollständiger Bericht erstellt werden kann.

Typ: Zeichenfolge

Zulässige Werte: PENDING | SUCCESS | ERROR

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

S3Config

Gibt den Amazon-Ressourcennamen (ARN) der AWS Identity and Access Management (IAM) -Rolle an, die für den Zugriff auf Ihren S3-Bucket DataSync verwendet wird.

Weitere Informationen finden Sie unter [DataSync Zugriff auf S3-Buckets bereitstellen](#).

Inhalt

BucketAccessRoleArn

Gibt den ARN der IAM-Rolle an, die für den Zugriff auf Ihren S3-Bucket DataSync verwendet wird.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

S3ManifestConfig

Gibt den S3-Bucket an, in dem Sie das Manifest hosten, das Sie verwenden AWS DataSync möchten. Weitere Informationen und Konfigurationsbeispiele finden Sie unter [Mithilfe eines Manifests angeben, welche DataSync Übertragungen übertragen](#) werden.

Inhalt

BucketAccessRoleArn

Gibt die AWS Identity and Access Management (IAM-) Rolle an, die DataSync den Zugriff auf Ihr Manifest ermöglicht. Weitere Informationen finden Sie unter [DataSync Zugriff auf Ihr Manifest bereitstellen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 2 048 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Erforderlich: Ja

ManifestObjectPath

Gibt den Amazon S3 S3-Objektschlüssel Ihres Manifests an. Dies kann ein Präfix enthalten (zum Beispielprefix/my-manifest.csv).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 4096.

Pattern: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Erforderlich: Ja

S3BucketArn

Gibt den Amazon-Ressourcennamen (ARN) des S3-Buckets an, in dem Sie Ihr Manifest hosten.

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 268.

Pattern: ^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:[a-z\\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\\-\\.]{1,63}\$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3-outposts:[a-z\\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\\-]{1,63}\$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9\\.\\-]{1,255}\$

Erforderlich: Ja

ManifestObjectVersionId

Gibt die Objektversions-ID des Manifests an, das Sie verwenden DataSync möchten. Wenn Sie dies nicht festlegen, DataSync wird die neueste Version des Objekts verwendet.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 100 Zeichen.

Pattern: ^.+\$

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SmbMountOptions

Gibt die Version des SMB-Protokolls (Server Message Block) an, das für den Zugriff auf einen SMB-Dateiserver AWS DataSync verwendet wird.

Inhalt

Version

Wählt standardmäßig DataSync automatisch eine SMB-Protokollversion auf der Grundlage der Verhandlungen mit Ihrem SMB-Dateiserver aus. Sie können auch die Verwendung einer bestimmten SMB-Version konfigurieren, aber wir empfehlen, dies nur dann DataSync zu tun, wenn Sie DataSync Probleme haben, automatisch mit dem SMB-Dateiserver zu verhandeln.

Dies sind die folgenden Optionen für die Konfigurierung der SMB-Version:

- **AUTOMATIC(Standard):** DataSync und der SMB-Dateiserver handeln zwischen 2.1 und 3.1.1 die höchste SMB-Version aus, die sie gegenseitig unterstützen.

Dies ist die empfohlene Option. Wenn Sie stattdessen eine bestimmte Version auswählen, die Ihr Dateiserver nicht unterstützt, erhalten Sie möglicherweise eine `Operation Not Supported`-Fehlermeldung.

- **SMB3:** Schränkt die Protokollverhandlung nur auf SMB-Version 3.0.2 ein.
- **SMB2:** Beschränkt die Protokollaushandlung nur auf SMB-Version 2.1.
- **SMB2_0:** Beschränkt die Protokollaushandlung nur auf SMB-Version 2.0.
- **SMB1:** Beschränkt die Protokollaushandlung nur auf SMB Version 1.0.

Note

Die SMB1 Option ist nicht verfügbar, wenn Sie [einen Amazon FSx for NetApp ONTAP-Standort erstellen](#).

Typ: Zeichenfolge

Zulässige Werte: AUTOMATIC | SMB2 | SMB3 | SMB1 | SMB2_0

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SourceManifestConfig

Gibt das Manifest an, das Sie verwenden AWS DataSync möchten, und wo es gehostet wird. Weitere Informationen und Konfigurationsbeispiele finden Sie unter [Mithilfe eines Manifests angeben, welche DataSync Übertragungen übertragen](#) werden.

Inhalt

S3

Gibt den S3-Bucket an, in dem Sie Ihr Manifest hosten.

Typ: [S3ManifestConfig](#) Objekt

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TagListEntry

Ein Schlüssel-Wert-Paar, das ein einzelnes Tag darstellt, das auf eine AWS Ressource angewendet wurde.

Inhalt

Key

Der Schlüssel für ein AWS Ressourcen-Tag.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:/-]+$`

Erforderlich: Ja

Value

Der Wert für ein AWS Ressourcen-Tag.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskExecutionFilesFailedDetail

Die Anzahl der Dateien oder Objekte, die DataSync während der Ausführung Ihrer Aufgabe nicht vorbereitet, übertragen, überprüft und gelöscht werden können.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Inhalt

Delete

Die Anzahl der Dateien oder Objekte, die DataSync während der Ausführung der Aufgabe nicht gelöscht werden konnten.

Type: Long

Erforderlich: Nein

Prepare

Die Anzahl der Dateien oder Objekte, die DataSync während der Ausführung der Aufgabe nicht vorbereitet werden konnten.

Type: Long

Erforderlich: Nein

Transfer

Die Anzahl der Dateien oder Objekte, die DataSync während der Ausführung der Aufgabe nicht übertragen werden konnten.

Type: Long

Erforderlich: Nein

Verify

Die Anzahl der Dateien oder Objekte, die DataSync während der Ausführung der Aufgabe nicht überprüft werden konnten.

Type: Long

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskExecutionFilesListedDetail

Die Anzahl der Dateien oder Objekte, die DataSync an Ihren Standorten gefunden wurden.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Inhalt

AtDestinationForDelete

Die Anzahl der Dateien oder Objekte, die DataSync an Ihrem Zielort gefunden wurden. Dieser Zähler gilt nur, wenn Sie [Ihre Aufgabe so konfigurieren](#), dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden.

Type: Long

Erforderlich: Nein

AtSource

Die Anzahl der Dateien oder Objekte, die an DataSync Ihrem Quellspeicherort gefunden wurden.

- DataSyncListet bei einem [Manifest](#) nur auf, was in Ihrem Manifest enthalten ist (und nicht alles, was sich an Ihrem Quellspeicherort befindet).
- Bei einem [Include-Filter](#) wird nur das DataSync aufgelistet, was dem Filter an Ihrem Quellspeicherort entspricht.
- DataSync Listet bei einem Ausschlussfilter alles auf, was sich an Ihrem Quellstandort befindet, bevor der Filter angewendet wird.

Type: Long

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskExecutionFoldersFailedDetail

Die Anzahl der Verzeichnisse, DataSync die während der Ausführung Ihrer Aufgabe nicht aufgelistet, vorbereitet, übertragen, verifiziert und gelöscht werden können.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Inhalt

Delete

Die Anzahl der Verzeichnisse, die DataSync während der Ausführung Ihrer Aufgabe nicht gelöscht werden konnten.

Type: Long

Erforderlich: Nein

List

Die Anzahl der Verzeichnisse, die DataSync während der Ausführung Ihrer Aufgabe nicht aufgelistet werden konnten.

Type: Long

Erforderlich: Nein

Prepare

Die Anzahl der Verzeichnisse, die DataSync während der Ausführung Ihrer Aufgabe nicht vorbereitet werden konnten.

Type: Long

Erforderlich: Nein

Transfer

Die Anzahl der Verzeichnisse, die DataSync während der Ausführung Ihrer Aufgabe nicht übertragen werden konnten.

Type: Long

Erforderlich: Nein

Verify

Die Anzahl der Verzeichnisse, die DataSync während der Ausführung Ihrer Aufgabe nicht überprüft werden konnten.

Type: Long

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskExecutionFoldersListedDetail

Die Anzahl der Verzeichnisse, die DataSync an Ihren Standorten gefunden wurden.

Note

Gilt nur für [Aufgaben im erweiterten Modus](#).

Inhalt

AtDestinationForDelete

Die Anzahl der Verzeichnisse, die DataSync an Ihrem Zielort gefunden wurden. Dieser Zähler ist nur relevant, wenn Sie [Ihre Aufgabe so konfigurieren](#), dass Daten im Ziel gelöscht werden, die sich nicht in der Quelle befinden.

Type: Long

Erforderlich: Nein

AtSource

Die Anzahl der Verzeichnisse, die DataSync an Ihrem Quellspeicherort gefunden wurden.

- DataSyncListet bei einem [Manifest](#) nur auf, was in Ihrem Manifest enthalten ist (und nicht alles an Ihrem Quellspeicherort).
- Bei einem [Include-Filter](#) wird nur das DataSync aufgelistet, was dem Filter an Ihrem Quellspeicherort entspricht.
- DataSync Listet bei einem Ausschlussfilter alles auf, was sich an Ihrem Quellstandort befindet, bevor der Filter angewendet wird.

Type: Long

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskExecutionListEntry

Stellt einen einzelnen Eintrag in einer Liste von AWS DataSync Aufgabenausführungen dar, der mit dem [ListTaskExecutions](#) Vorgang zurückgegeben wird.

Inhalt

Status

Der Status einer Aufgabenausführung. Weitere Informationen finden Sie unter [Status der Aufgabenausführung](#).

Typ: Zeichenfolge

Zulässige Werte: QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING
| VERIFYING | SUCCESS | ERROR

Erforderlich: Nein

TaskExecutionArn

Der Amazon-Ressourcenname (ARN) einer Aufgabenausführung.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Erforderlich: Nein

TaskMode

Der Aufgabenmodus, den Sie verwenden. Weitere Informationen finden Sie unter [Auswählen eines Aufgabenmodus für Ihre Datenübertragung](#).

Typ: Zeichenfolge

Zulässige Werte: BASIC | ENHANCED

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskExecutionResultDetail

Stellt detaillierte Informationen über das Ergebnis Ihrer AWS DataSync Aufgabenausführung bereit.

Inhalt

ErrorCode

Ein Fehler, der während der Ausführung Ihrer Aufgabe DataSync aufgetreten ist. Sie können diese Informationen verwenden, um [Probleme zu beheben](#).

Typ: Zeichenfolge

Erforderlich: Nein

ErrorDetail

Die ausführliche Beschreibung eines Fehlers, der bei der Ausführung Ihrer Aufgabe DataSync aufgetreten ist. Sie können diese Informationen verwenden, um [Probleme zu beheben](#).

Typ: Zeichenfolge

Erforderlich: Nein

PrepareDuration

Die Zeit in Millisekunden, in der Ihre Aufgabe in dem Schritt ausgeführt wurde. PREPARING
Weitere Informationen finden Sie unter Status der [Aufgabenausführung](#).

Für Aufgaben im erweiterten Modus ist der Wert immer 0. Weitere Informationen finden Sie unter [So wird Ihre Datenübertragung DataSync vorbereitet](#).

Type: Long

Gültiger Bereich: Mindestwert 0.

Erforderlich: Nein

PrepareStatus

Der Status des PREPARING Schritts für die Ausführung Ihrer Aufgabe. Weitere Informationen finden Sie unter [Status der Aufgabenausführung](#).

Typ: Zeichenfolge

Zulässige Werte: PENDING | SUCCESS | ERROR

Erforderlich: Nein

TotalDuration

Die Zeit in Millisekunden, in der Ihre Aufgabenausführung ausgeführt wurde.

Type: Long

Gültiger Bereich: Mindestwert 0.

Erforderlich: Nein

TransferDuration

Die Zeit in Millisekunden, in der Ihre Aufgabe in dem Schritt ausgeführt wurde. TRANSFERRING
Weitere Informationen finden Sie unter Status der [Aufgabenausführung](#).

Für Aufgaben im erweiterten Modus ist der Wert immer 0. Weitere Informationen finden Sie unter [So werden Ihre Daten DataSync übertragen](#).

Type: Long

Gültiger Bereich: Mindestwert 0.

Erforderlich: Nein

TransferStatus

Der Status des TRANSFERRING Schritts für Ihre Aufgabenausführung. Weitere Informationen finden Sie unter [Status der Aufgabenausführung](#).

Typ: Zeichenfolge

Zulässige Werte: PENDING | SUCCESS | ERROR

Erforderlich: Nein

VerifyDuration

Die Zeit in Millisekunden, zu der Ihre Aufgabe in dem Schritt ausgeführt wurde. VERIFYING
Weitere Informationen finden Sie unter Status der [Aufgabenausführung](#).

Für Aufgaben im erweiterten Modus ist der Wert immer 0. Weitere Informationen finden Sie unter [So wird die Integrität Ihrer Daten DataSync überprüft](#).

Type: Long

Gültiger Bereich: Mindestwert 0.

Erforderlich: Nein

VerifyStatus

Der Status des VERIFYING Schritts für die Ausführung Ihrer Aufgabe. Weitere Informationen finden Sie unter [Status der Aufgabenausführung](#).

Typ: Zeichenfolge

Zulässige Werte: PENDING | SUCCESS | ERROR

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskFilter

Sie können API-Filter verwenden, um die Liste der von zurückgegebenen Ressourcen einzugrenzen `ListTasks`. Um beispielsweise alle Aufgaben an einem Quellspeicherort abzurufen, können Sie dies `ListTasks` mit dem Filternamen `LocationId` und Operator `Equals` mit dem ARN für den Speicherort verwenden.

Weitere Informationen finden Sie unter [DataSyncRessourcen filtern](#).

Inhalt

Name

Der Name des verwendeten Filters. Jeder API-Aufruf unterstützt eine Liste von Filtern, die für ihn verfügbar sind. Beispielsweise `LocationId` für `ListTasks`.

Typ: Zeichenfolge

Zulässige Werte: `LocationId` | `CreationTime`

Erforderlich: Ja

Operator

Der Operator, der zum Vergleichen von Filterwerten verwendet wird (z. B. `Equals` oder `Contains`).

Typ: Zeichenfolge

Zulässige Werte: `Equals` | `NotEquals` | `In` | `LessThanOrEqual` | `LessThan` | `GreaterThanOrEqual` | `GreaterThan` | `Contains` | `NotContains` | `BeginsWith`

Erforderlich: Ja

Values

Die Werte, nach denen Sie filtern möchten. Beispielsweise möchten Sie möglicherweise nur Aufgaben für einen bestimmten Zielort anzeigen.

Typ: Zeichenfolgen-Array

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Pattern: `^[0-9a-zA-Z_\ \-\:\*\.\ \\/\?\-]*$`

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskListEntry

Stellt einen einzelnen Eintrag in einer Aufgabenliste dar. TaskListEntry gibt ein Array zurück, das eine Liste von Aufgaben enthält, wenn die [ListTasks](#) Operation aufgerufen wird. Eine Aufgabe umfasst die zu synchronisierenden Quell- und Zieldateisysteme sowie die für die Aufgaben zu verwendenden Optionen.

Inhalt

Name

Der Name der -Aufgabe.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Erforderlich: Nein

Status

Der Status der Aufgabe.

Typ: Zeichenfolge

Zulässige Werte: AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE

Erforderlich: Nein

TaskArn

Der Amazon-Ressourcenname (ARN) der Aufgabe.

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 128 Zeichen.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erforderlich: Nein

TaskMode

Der Aufgabenmodus, den Sie verwenden. Weitere Informationen finden Sie unter [Auswählen eines Aufgabenmodus für Ihre Datenübertragung](#).

Typ: Zeichenfolge

Zulässige Werte: BASIC | ENHANCED

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskReportConfig

Gibt an, wie Sie einen Aufgabenbericht konfigurieren möchten, der detaillierte Informationen zu Ihrer AWS DataSync Übertragung enthält.

Weitere Informationen finden Sie unter [Aufgabenberichte](#).

Inhalt

Destination

Gibt den Amazon S3 S3-Bucket an, in den Ihr Aufgabenbericht DataSync hochgeladen wird. Weitere Informationen finden Sie unter [Aufgabenberichte](#).

Typ: [ReportDestination](#) Objekt

Erforderlich: Nein

ObjectVersionIds

Gibt an, ob Ihr Aufgabenbericht die neue Version jedes Objekts enthält, das in einen S3-Bucket übertragen wurde. Dies gilt nur, wenn Sie die [Versionierung für Ihren Bucket aktivieren](#). Denken Sie daran, dass die Dauer Ihrer Aufgabenausführung verlängert INCLUDE werden kann, wenn Sie diesen Wert auf festlegen.

Typ: Zeichenfolge

Zulässige Werte: INCLUDE | NONE

Erforderlich: Nein

OutputType

Gibt den Typ des gewünschten Aufgabenberichts an:

- SUMMARY_ONLY: Stellt die erforderlichen Details zu Ihrer Aufgabe bereit, einschließlich der Anzahl der übertragenen Dateien, Objekte und Verzeichnisse sowie der Übertragungsdauer.
- STANDARD: Enthält vollständige Details zu Ihrer Aufgabe, einschließlich einer vollständigen Liste der Dateien, Objekte und Verzeichnisse, die übertragen, übersprungen, verifiziert wurden und mehr.

Typ: Zeichenfolge

Zulässige Werte: SUMMARY_ONLY | STANDARD

Erforderlich: Nein

Overrides

Passt die Berichtsebene für Aspekte Ihres Aufgabenberichts an. Beispielsweise könnte Ihr Bericht im Allgemeinen nur Fehler enthalten, aber Sie könnten angeben, dass Sie eine Liste mit Erfolgen und Fehlern nur für die Dateien wünschen, die DataSync versucht wurden, an Ihrem Zielort zu löschen.

Typ: [ReportOverrides](#) Objekt

Erforderlich: Nein

ReportLevel

Gibt an, ob Ihr Aufgabenbericht nur die Fehler bei der Übertragung oder eine Liste der erfolgreichen und nicht erfolgreichen Übertragungen enthalten soll.

- **ERRORS_ONLY:** In einem Bericht wird angezeigt, DataSync was nicht übertragen, übersprungen, verifiziert und gelöscht werden konnte.
- **SUCCESSES_AND_ERRORS:** Ein Bericht zeigt, DataSync was übertragen, übersprungen, verifiziert und gelöscht werden konnte und was nicht.

Typ: Zeichenfolge

Zulässige Werte: **ERRORS_ONLY** | **SUCCESSES_AND_ERRORS**

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskSchedule

Konfiguriert Ihre AWS DataSync Aufgabe so, dass sie nach einem [Zeitplan](#) ausgeführt wird (in einem Mindestintervall von 1 Stunde).

Inhalt

ScheduleExpression

Gibt Ihren Task-Zeitplan mithilfe eines Cron- oder Rate-Ausdrucks an.

Verwenden Sie Cron-Ausdrücke für Aufgabenpläne, die zu einer bestimmten Uhrzeit und an einem bestimmten Tag ausgeführt werden. Mit dem folgenden Cron-Ausdruck wird beispielsweise ein Aufgabenplan erstellt, der jeden ersten Mittwoch im Monat um 8 Uhr ausgeführt wird:

```
cron(0 8 * * 3#1)
```

Verwenden Sie Ratenausdrücke für Aufgabenpläne, die in regelmäßigen Abständen ausgeführt werden. Mit dem folgenden Ratenausdruck wird beispielsweise ein Aufgabenplan erstellt, der alle 12 Stunden ausgeführt wird:

```
rate(12 hours)
```

Informationen zur Syntax von Cron- und Rate-Ausdrücken finden Sie im [EventBridge Amazon-Benutzerhandbuch](#).

Typ: Zeichenfolge

Längenbeschränkungen: Maximale Länge beträgt 256 Zeichen.

Pattern: `^[a-zA-Z0-9\ \_\*\?\,\|\^\-\/\#\s\(\)\+]*$`

Erforderlich: Ja

Status

Gibt an, ob Ihr Aufgabenplan aktiviert oder deaktiviert werden soll. Ihr Zeitplan ist standardmäßig aktiviert, aber es kann Situationen geben, in denen Sie ihn deaktivieren müssen. Beispielsweise müssen Sie möglicherweise eine wiederkehrende Übertragung unterbrechen, um ein Problem mit Ihrer Aufgabe zu beheben oder Wartungsarbeiten an Ihrem Speichersystem durchzuführen.

DataSync deaktiviert Ihren Zeitplan möglicherweise automatisch, wenn Ihre Aufgabe wiederholt mit demselben Fehler fehlschlägt. Weitere Informationen finden Sie unter [TaskScheduleDetails](#).

Typ: Zeichenfolge

Zulässige Werte: ENABLED | DISABLED

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TaskScheduleDetails

Stellt Informationen zu Ihrem AWS DataSync [Aufgabenplan](#) bereit.

Inhalt

DisabledBy

Zeigt an, wie Ihr Taskplan deaktiviert wurde.

- USER- Ihr Zeitplan wurde manuell mithilfe der [UpdateTask](#) Operation oder der DataSync Konsole deaktiviert.
- SERVICE- Ihr Zeitplan wurde automatisch deaktiviert DataSync, weil die Aufgabe wiederholt mit demselben Fehler fehlschlug.

Typ: Zeichenfolge

Zulässige Werte: USER | SERVICE

Erforderlich: Nein

DisabledReason

Gibt einen Grund an, warum der Taskplan deaktiviert ist.

Wenn Ihr Zeitplan von deaktiviert istUSER, wird eine `Manually disabled by user`. Meldung angezeigt.

Wenn Ihr Zeitplan von deaktiviert istSERVICE, wird Ihnen eine Fehlermeldung angezeigt, die Ihnen hilft zu verstehen, warum die Aufgabe immer wieder fehlschlägt. Informationen zur Behebung von DataSync Fehlern finden Sie unter [Problembehandlung bei DataSync Übertragungen](#).

Typ: Zeichenfolge

Längenbeschränkungen: Die maximale Länge beträgt 8192.

Pattern: `^[\\w\\s.,'?!:;\\/=|<>()-]*$`

Erforderlich: Nein

StatusUpdateTime

Gibt an, wann sich der Status Ihres Taskplans das letzte Mal geändert hat. Wenn Ihr Zeitplan beispielsweise aufgrund eines wiederholten Fehlers DataSync automatisch deaktiviert wird, können Sie sehen, wann der Zeitplan deaktiviert wurde.

Typ: Zeitstempel

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Häufige Fehler

In diesem Abschnitt werden die Fehler aufgeführt, die bei den API-Aktionen aller AWS Dienste häufig auftreten. Informationen zu Fehlern, die spezifisch für eine API-Aktion für diesen Service sind, finden Sie unter dem Thema für diese API-Aktion.

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

HTTP Status Code: 400

IncompleteSignature

Die Anforderungssignatur entspricht nicht den AWS Standards.

HTTP Status Code: 400

InternalFailure

Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.

HTTP Status Code: 500

InvalidAction

Die angeforderte Aktion oder Operation ist ungültig. Überprüfen Sie, ob die Aktion ordnungsgemäß eingegeben wurde.

HTTP Status Code: 400

InvalidClientTokenId

Das angegebene X.509-Zertifikat oder die angegebene AWS Zugriffsschlüssel-ID ist in unseren Aufzeichnungen nicht vorhanden.

HTTP Status Code: 403

NotAuthorized

Sie haben keine Berechtigung zum Ausführen dieser Aktion.

HTTP Status Code: 400

OptInRequired

Für die AWS Zugriffsschlüssel-ID ist ein Abonnement für den Dienst erforderlich.

HTTP Status Code: 403

RequestExpired

Die Anfrage erreichte den Service mehr als 15 Minuten nach dem Datumsstempel auf der Anfrage oder mehr als 15 Minuten nach dem Ablaufdatum der Anfrage (z. B. bei vorsignierter Anfrage URLs), oder der Datumsstempel auf der Anfrage liegt mehr als 15 Minuten in der future.

HTTP Status Code: 400

ServiceUnavailable

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 503

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

HTTP Status Code: 400

ValidationError

Die Eingabe erfüllt nicht die von einem AWS Dienst angegebenen Einschränkungen.

HTTP Status Code: 400

Geläufige Parameter

Die folgende Liste enthält die Parameter, die alle Aktionen zum Signieren von Signature-Version-4-Anforderungen mit einer Abfragezeichenfolge verwenden. Alle aktionsspezifischen Parameter werden im Thema für diese Aktion aufgelistet. Weitere Informationen zu Signature Version 4 finden Sie unter [Signieren von AWS API-Anfragen](#) im IAM-Benutzerhandbuch.

Action

Die auszuführende Aktion.

Typ: Zeichenfolge

Erforderlich: Ja

Version

Die API-Version, für die die Anfrage geschrieben wurde, ausgedrückt im Format YYYY-MM-DD.

Typ: Zeichenfolge

Erforderlich: Ja

X-Amz-Algorithm

Der Hashalgorithmus, den Sie zum Erstellen der Anforderungssignatur verwendet haben.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Zulässige Werte: AWS4-HMAC-SHA256

Required: Conditional

X-Amz-Credential

Der Wert des Anmeldeinformationsumfangs. Dabei handelt es sich um eine Zeichenfolge, die Ihren Zugriffsschlüssel, das Datum, die gewünschte Region und eine Zeichenfolge zur Beendigung („aws4_request“) beinhaltet. Der Wert wird im folgenden Format ausgedrückt: Zugriffsschlüssel/JJJJMMTT/Region/Service/aws4_request.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erstellen einer signierten AWS API-Anfrage](#).

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Date

Das Datum, das zum Erstellen der Signatur verwendet wird. Das Format muss das ISO 8601-Basisformat (JJJJMMTT'T'SSMMSS'Z') sein. Beispielsweise ist die folgende Datums- und Uhrzeitangabe ein gültiger X-Amz-Date Wert:20120325T120000Z.

Bedingung: X-Amz-Date ist bei allen Anforderungen optional. Damit kann das Datum überschrieben werden, das zum Signieren von Anforderungen verwendet wird. Wenn der Date-Header im ISO 8601-Grundformat angegeben ist, X-Amz-Date ist dies nicht erforderlich.

Wenn verwendet X-Amz-Date wird, überschreibt er immer den Wert des Date-Headers.

Weitere Informationen finden Sie unter [Elemente einer AWS API-Anforderungssignatur](#) im IAM-Benutzerhandbuch.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Security-Token

Das temporäre Sicherheitstoken, das durch einen Aufruf von AWS -Security-Token-Service (AWS STS) abgerufen wurde. Eine Liste der Services, die temporäre Sicherheits-Anmeldeinformationen von AWS STS unterstützen, finden Sie im IAM-Benutzerhandbuch unter [AWS-Services , die mit IAM funktionieren](#).

Bedingung: Wenn Sie temporäre Sicherheitsanmeldedaten von verwenden AWS STS, müssen Sie das Sicherheitstoken angeben.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Signature

Gibt die hex-codierte Signatur an, die aus der zu signierenden Zeichenfolge und dem abgeleiteten Signaturschlüssel berechnet wurde.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-SignedHeaders

Gibt alle HTTP-Header an, die als Teil der kanonischen Anforderung enthalten waren. Weitere Informationen zur Angabe signierter Header finden Sie unter [Erstellen einer signierten AWS API-Anfrage](#) im IAM-Benutzerhandbuch.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

Dokumentverlauf

In der folgenden Tabelle werden wichtige Ergänzungen der AWS DataSync Dokumentation beschrieben. Wir aktualisieren die Dokumentation auch regelmäßig, um auf Ihr Feedback einzugehen.

Abonnieren Sie den RSS-Feed, um über Aktualisierungen dieser Dokumentation informiert zu werden.

Änderung	Beschreibung	Datum
Support für VPC-Endpunktrichtlinien und FIPS-fähige VPC-Endpunkte hinzugefügt	Sie können jetzt VPC-Endpunktrichtlinien verwenden und FIPS-VPC-Endpunkte in FIPS-fähig auswählen. AWS-Regionen	30. September 2025
Support für IPv6 Adressen hinzugefügt	Sie können jetzt IPv6 Adressen verwenden IPv4 , um eine Verbindung mit DataSync und für Datenübertragungen mit unterstützten Datenquellen herzustellen.	16. Juli 2025
Discovery ist nicht mehr verfügbar	Ab dem 20. Mai 2025 ist Discovery nicht mehr DataSync verfügbar.	20. Mai 2025
AWS verwaltetes Richtlinienupdate — Aktualisierung der bestehenden Richtlinie	Die AWSDataSyncFullAccess Richtlinie enthält aktualisierte Berechtigungsanweisungen, die Tagging-Bedingungen aus den Berechtigungen entfernen , die zum Erstellen von Secrets Manager Manager-	13. Mai 2025

Geheimnissen DataSync verwendet werden.

[AWS verwaltetes Richtlini
enupdate — Aktualisierung der
bestehenden Richtlinie](#)

Die AWSDatasyncFullAccess Richtlinie verfügt über neue Berechtigungen, mit denen DataSync Sie arbeiten können AWS Secrets Manager.

7. Mai 2025

[AWS verwaltetes Richtlini
enupdate — Aktualisierung der
bestehenden Richtlinie](#)

Die AWSDatasyncFullAccess Richtlinie verfügt über neue Berechtigungen, mit denen DataSync Sie arbeiten können AWS Secrets Manager.

23. April 2025

[AWS verwaltetes Richtlini
enupdate — Aktualisierung der
bestehenden Richtlinie](#)

Die AWSDatasyncFullAccess Richtlinie verfügt über neue Berechtigungen, die DataSync das Arbeiten mit AWS Secrets Manager und ermöglichen AWS Key Management Service.

23. April 2025

[AWS verwaltetes Richtlini
enupdate — Aktualisierung der
bestehenden Richtlinie](#)

Das AWSDatasyncServiceRolePolicy hat neue Berechtigungen, mit DataSync denen gearbeitet werden kann AWS Secrets Manager.

15. April 2025

[Durchführung großer
Datenmigrationen](#)

Erfahren Sie, wie Sie groß angelegte Datenmigrationen planen, indem Sie DataSync Dateien oder Objekte von lokalen oder anderen Cloud-Speichern in übertragen. AWS

19. Februar 2025

Support für Kerberos mit SMB-Standorten	DataSync kann jetzt die Kerberos-Authentifizierung verwenden, wenn eine Verbindung zu SMB-Dateiservern (Server Message Block) hergestellt wird.	28. Januar 2025
Neu AWS-Region	AWS DataSync ist für Datenübertragungen in der Region Mexiko (Zentral) verfügbar.	14. Januar 2025
Neu AWS-Region	AWS DataSync ist für Datenübertragungen in der Region Asien-Pazifik (Thailand) verfügbar.	7. Januar 2025
AWS Speicherorte aktualisieren	Sie können jetzt Ihre Amazon S3-, Amazon EFS- und FSx Amazon-Transferstandorte aktualisieren.	18. Dezember 2024
Snowball Edge wird nicht mehr unterstützt	Wird ab dem 12. November 2024 nicht DataSync mehr unterstützt AWS Snowball Edge.	13. November 2024
Neue AWS verwaltete Richtlinie	Die angegebene DataSync dienstbezogene Rolle <code>AWSServiceRoleForDataSync</code> verwendet eine neue verwaltete Richtlinie mit dem Namen <code>AWSDataSyncServiceRolePolicy</code> .	30. Oktober 2024

Wir stellen vor: Erweiterter Modus	Im erweiterten Modus können Sie eine praktisch unbegrenzte Anzahl von Objekten zwischen Amazon S3 S3-Standorten übertragen.	30. Oktober 2024
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Die AWSDataSyncFullAccess Richtlinie enthält eine neue Berechtigung für Dienste, die mit arbeiten DataSync.	30. Oktober 2024
Support für allgemeine Azure Speicherkonten der Version 1	DataSync kann bei der Übertragung zu oder von Azure dort mit Allzweck-Speicherkonten der Version 1 verwendet werden. Microsoft Azure Blob Storage	4. Oktober 2024
Neue Methode zur Konfiguration von Task-Zeitplänen	Sie können Ihre DataSync Aufgabenpläne mithilfe von Ratenausdrücken konfigurieren.	22. August 2024
Neu AWS-Region	AWS DataSync ist für Datenübertragungen in der Region Asien-Pazifik (Malaysia) verfügbar.	21. August 2024
Support für agentenlose regionsübergreifende Übertragungen, die eine Opt-in-Region beinhalten	Sie benötigen keinen DataSync Agenten mehr für Übertragungen zwischen AWS Speicherdiensten, wenn mindestens ein Speicherort aktiviert ist. AWS-Region	24. Juli 2024

AWS verwaltete Richtlini enaktualisierungen — Aktualisi erung einer bestehenden Richtlinie	Die AWSDataSyncFullAcc ess Richtlinie enthält eine neue Berechtigung für Dienste, die mit arbeiten DataSync.	22. Juli 2024
Das S3-Kontoübergreifendes Tutorial wurde aktualisiert	Einige Benutzerberechtigu ngen für Quellkonten, die für diese Übertragung nicht mehr erforderlich sind, wurden entfernt.	10. Juni 2024
Neuer Status der Aufgabena usführung	Der CANCELLING Status gibt an, wann eine Aufgabena usführung abgebrochen wird.	15. Mai 2024
Neue Option zum Pausieren von Task-Zeitplänen	Sie können Ihren AWS DataSync Task-Zeitplan deaktivieren, wenn Sie Probleme beheben oder das Speichersystem warten müssen.	24. April 2024
Die TLS-Chiffre für FIPS-Endp unkte wurde aktualisiert	AWS DataSync verwendet die Verschlüsselung TLS_AES_1 28_GCM_SHA256 (secp256r 1) für FIPS-Dienstendpunkte (Federal Information Processin g Standard).	22. April 2024
AWS verwaltete Richtlini enaktualisierungen — Aktualisi erung einer vorhandenen Richtlinie	Die AWSDataSyncFullAcc ess Richtlinie enthält eine neue Berechtigung für Dienste, die mit arbeiten DataSync.	16. Februar 2024

<u>Übertragen Sie bestimmte Dateien oder Objekte mit einem Manifest</u>	AWS DataSync kann eine Liste von Dateien oder Objekten mithilfe eines Manifests übertragen.	7. Februar 2024
<u>Neu AWS-Region</u>	AWS DataSync ist jetzt für Datenübertragungen in der Region Kanada West (Calgary) verfügbar.	20. Dezember 2023
<u>Support für Übertragungen mit zusätzlichen Cloud-Anbietern</u>	AWS DataSync kann jetzt Daten zwischen AWS Speicherdiensten und IBM Cloud Object Storage oder übertragenSeagate Lyve Cloud.	7. November 2023
<u>Support für Übertragungen mit Alibaba Cloud Object Storage Service</u>	AWS DataSync kann jetzt Daten zwischen AWS Speicherdiensten und übertragenAlibaba Cloud Object Storage Service.	25. September 2023
<u>Support für Aufgabenberichte</u>	Überwachen Sie Ihre AWS DataSync Übertragungen mit Aufgabenberichten.	30. August 2023
<u>Neu AWS-Region</u>	AWS DataSync ist jetzt für Datenübertragungen in der Region Israel (Tel Aviv) verfügbar.	23. August 2023

<u>Support für Übertragungen mit zusätzlichen Cloud-Anbietern</u>	AWS DataSync kann jetzt Daten zwischen AWS Speicherdiensten und mehreren anderen Cloud-Anbietern (wie Wasabi Cloud Storage, DigitalOcean Spaces, und Oracle Cloud Infrastructure Object Storage) übertragen.	08. August 2023
<u>Allgemeine Verfügbarkeit des Microsoft Azure Blob Storage Supports</u>	AWS DataSync kann jetzt Objekte hin und von dort übertragen Microsoft Azure Blob Storage.	25. Juli 2023
<u>Unterstützung für TLS 1.3</u>	Bei der Übertragung zwischen Speicherorten wird AWS DataSync jetzt der gesamte Netzwerkverkehr mit Transport Layer Security (TLS) 1.3 verschlüsselt.	28. Juni 2023
<u>Neue DataSync Discovery-Metriken</u>	AWS DataSync Discovery kann Ihnen jetzt sagen, wie viele LUNs (logische Einheiten nummern) sich in einem Speicherressourcen-Cluster, einer virtuellen Speichermaschine (SVM) oder einem Volume befinden.	28. Juni 2023
<u>Neu AWS-Region</u>	AWS DataSync ist jetzt für Datenübertragungen in der Region Asien-Pazifik (Melbourne) verfügbar.	24. Mai 2023

Support für S3-kompatiblen Speicher auf Snowball Edge	Sie können AWS DataSync verwenden, um Daten zwischen Amazon S3 S3-kompatiblen Speicherdiensten AWS Snowball Edge und AWS Speicherdiensten zu übertragen.	18. Mai 2023
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Die <code>AWSDatasyncFullAccess</code> Richtlinie enthält neue Berechtigungen für Dienste, die mit arbeiten DataSync.	2. Mai 2023
Allgemeine Verfügbarkeit von AWS DataSync Discovery	Verwenden Sie DataSync Discovery, um Ihre Migration zu zu beschleunigen AWS.	25. April 2023
Öffentliche Vorschauversion der Microsoft Azure Blob Storage-Unterstützung	AWS DataSync kann jetzt Objekte von Microsoft Azure Blob Storage übertragen.	29. März 2023
Neue IAM-Richtlinie	DataSync Verwendet zur Unterstützung der DataSync Discovery-Funktion die mit dem Dienst verknüpfte Rolle mit dem Namen <code>AWSServiceRoleForDataSyncDiscovery</code> .	21. März 2023
Neu AWS-Regionen	AWS DataSync ist jetzt in den folgenden Ländern erhältlich AWS-Regionen: Asien-Pazifik (Hyderabad), Europa (Spanien) und Europa (Zürich).	06. Februar 2023

Verwendung von Tags bei der Ausführung von Aufgaben	Sie können Ihre AWS DataSync Aufgabena usführungen jetzt taggen.	16. Dezember 2022
Support für S3 Glacier Instant Retrieval	Sie können jetzt Objekte direkt in die Speicherklasse S3 Glacier Instant Retrieval übertragen.	16. Dezember 2022
Objektsystem-Metadaten werden kopiert	AWS DataSync kann jetzt Systemmetadaten bei der Übertragung zwischen einem Objektspeichersystem und Amazon S3 kopieren.	16. Dezember 2022
Neu AWS-Regionen	AWS DataSync ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar.	14. Dezember 2022
Neu AWS-Region	AWS DataSync ist jetzt in der Region Naher Osten (VAE) verfügbar.	16. November 2022
Support für selbstsignierte Zertifikate mit Objektspeicherorten	AWS DataSync kann eine Verbindung zu Objektspeicherorten herstellen, die selbstsignierte oder private Zertifikate verwenden.	25. Oktober 2022
Informationen zur Datenkomprimierung abrufen	AWS DataSync kann die physische Anzahl der Byte angeben, die nach der Komprimierung über das Netzwerk übertragen wurden.	25. Oktober 2022
Öffentliche Vorschauversion von AWS DataSync Discovery	Verwenden Sie DataSync Discovery, um Ihre Migration zu zu beschleunigen AWS.	21. September 2022

Neue Option für die Migration von Daten zu oder von Google Cloud Storage	Sie können Daten zu oder von Google Cloud Storage übertragen, indem Sie einen AWS DataSync Agenten in Google Cloud bereitstellen.	21. Juli 2022
Support für Amazon FSx für NetApp ONTAP-Dateisysteme	AWS DataSync kann jetzt Dateien und Ordner von FSx und zu ONTAP-Dateisystemen übertragen.	28. Juni 2022
Neue Sicherheitsoptionen für Amazon EFS-Standorte	AWS DataSync kann mithilfe von TLS, Access Points und IAM-Rollen auf Amazon EFS-Dateisysteme zugreifen.	31. Mai 2022
Daten zu oder von Google Cloud Storage und Azure Files migrieren	Mit AWS DataSync können Sie Daten zu oder von Google Cloud Storage und Azure Files übertragen. Weitere Informationen finden Sie unter Erstellen eines Speichers für Objektspeicher und Erstellen eines Speicherorts für SMB .	24. Mai 2022
Neue AWS DataSync Aufgabeneinstellung	Mit der Option Objekt-Tags kopieren können Sie angeben, ob Objekt-Tags bei der Übertragung zwischen Objektspeichersystemen beibehalten werden sollen.	5. Mai 2022
Neu AWS-Region	AWS DataSync ist jetzt in der Region Asien-Pazifik (Jakarta) verfügbar.	19. April 2022

<u>Support für Amazon FSx für OpenZFS-Dateisysteme</u>	AWS DataSync kann jetzt Dateien und Ordner von und zu FSx OpenZFS-Dateisystemen übertragen.	5. April 2022
<u>Support für Amazon FSx for Lustre-Dateisysteme</u>	AWS DataSync kann jetzt Dateien und Ordner von FSx und zu Lustre-Dateisystemen übertragen.	10. Dezember 2021
<u>Support für Hadoop Distributed File Systems (HDFS)</u>	AWS DataSync unterstützt jetzt die Übertragung von Dateien und Ordnern zu und von HDFS-Clustern.	3. November 2021
<u>Neu AWS-Region</u>	AWS DataSync ist jetzt in der Region Asien-Pazifik (Osaka) verfügbar.	28. Juli 2021
<u>Vollautomatische Übertragungen zwischen AWS Speicherdiensten</u>	AWS DataSync kann jetzt mit nur wenigen Klicks in der DataSync Konsole Dateien oder Objekte zwischen Amazon S3, Amazon EFS oder FSx für Windows File Server übertragen.	9. November 2020
<u>Anpassen der Netzwerkbandbreite, die von einer laufenden Aufgabe verwendet wird</u>	AWS DataSync ermöglicht es Kunden jetzt, die Netzwerkbandbreite anzupassen, die von einer laufenden DataSync Aufgabe verwendet wird. Dies trägt dazu bei, die Auswirkungen auf andere Benutzer oder Anwendungen zu minimieren, wenn sich eine Aufgabe über mehrere Tage erstreckt.	9. November 2020

[Verbesserte Unterstützung für lokale Funktionen DataSync virtueller Maschinen \(VM\)](#)

Die AWS DataSync Agenten-VM-Hostkonsole unterstützt jetzt erweiterte Funktionen, einschließlich der Aktivierung eines Agenten von der lokalen Konsole aus.

19. Oktober 2020

[AWS DataSync kann jetzt Daten von und zu übertragen AWS Outposts](#)

DataSync unterstützt jetzt die Übertragung von Objekten zu und von Amazon S3 AWS Outposts.

30. September 2020

[Support für API-Filterung](#)

AWS DataSync unterstützt jetzt das Filtern nach Aufrufen `ListTasks` und `ListLocations` API-Aufrufen, sodass Sie die Konfiguration von Datenübertragungsaufgaben einfach abrufen können, indem Sie Filter wie die Quelle oder das Ziel für die Datenübertragung verwenden.

18. August 2020

[Support für das Kopieren von Daten aus Ihrem selbstverwalteten Objektspeicher](#)

AWS DataSync unterstützt jetzt die Datenübertragung zwischen selbstverwaltetem Objektspeicher und Amazon S3, Amazon Elastic File System oder FSx für Windows File Server.

27. Juli 2020

[Support für Linux-Kernel-basierte virtuelle Maschinen \(KVM\) und Microsoft Hyper-V-Hypervisoren](#)

AWS DataSync bietet jetzt zusätzlich zu den bestehenden VMware und Amazon-Optionen die Möglichkeit, lokale Agenten auf den KVM- und Microsoft Hyper-V-Virtualisierungsplattformen bereitzustellen. EC2

1. Juli 2020

[AWS DataSync kann jetzt Ihre Amazon CloudWatch Logs-Konfiguration automatisch konfigurieren](#)

Bei der Nutzung haben Sie jetzt die Möglichkeit DataSync, automatisch die CloudWatch Protokollgruppe und die Ressourcenrichtlinie zu generieren, die für die Veröffentlichung von Protokollen für Ihre Datenübertragung erforderlich sind, was die Erstellung von Aufgaben und die Einrichtung der Überwachung vereinfacht.

1. Juli 2020

[AWS DataSync kann jetzt Daten von und zu übertragen AWS Snowball Edge](#)

DataSync unterstützt jetzt die Übertragung von Dateien zu und von AWS Snowball Edge, dem kleinsten Mitglied AWS Snow Family der Edge-Computing- und Datenübertragungsgeräte. Snowball Edge ist tragbar, robust und sicher — klein und leicht genug, um in einen Rucksack zu passen und rauen Umgebungen standzuhalten.

17. Juni 2020

<u>Neu AWS-Region</u>	AWS DataSync ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar.	16. Juni 2020
<u>Verbesserte Überwachungsfunktionen mit Protokollierung auf Dateiebene</u>	Sie können jetzt die detaillierte Protokollierung für Dateien und Objekte aktivieren, die zwischen Ihren NFS-Servern, SMB-Servern, Amazon S3 S3-Buckets, Amazon EFS-Dateisystemen und FSx für Windows File Server-Dateisysteme kopiert wurden.	24. April 2020
<u>Support für das Kopieren von Daten zwischen Ihrem SMB-Share und Amazon FSx for Windows File Server</u>	Sie können jetzt Daten zwischen Ihrer SMB-Freigabe und dem FSx Windows-Dateiserver kopieren.	24. Januar 2020
<u>Support für die Planung von Aufgaben</u>	Sie können ab sofort Aufgaben manuell ausführen oder planen, dass sie basierend auf einem angegebenen Zeitplans ausgeführt werden.	20. November 2019
<u>Neu AWS-Region</u>	AWS DataSync ist jetzt in den Regionen Asien-Pazifik (Hongkong), Asien-Pazifik (Mumbai), Europa (Stockholm), Südamerika (São Paulo) und AWS GovCloud (USA-Ost) verfügbar.	20. November 2019

<u>Neu AWS-Region</u>	AWS DataSync ist jetzt in den Regionen Kanada (Zentral), Europa (London) und Europa (Paris) verfügbar.	2. Oktober 2019
<u>Support für Amazon S3 S3-Speicherklassen</u>	Sie können jetzt Objekte direkt in Amazon S3 S3-Speicherklassen übertragen.	24. September 2019
<u>Neu AWS-Region</u>	AWS DataSync ist jetzt in der Region Naher Osten (Bahrain) verfügbar.	28. August 2019
<u>Support für das Kopieren von Daten zwischen Ihrer Server Message Block (SMB) -Share und Amazon S3 oder Amazon EFS</u>	Sie können jetzt Daten zwischen Ihrer SMB-Dateifreigabe und Amazon S3 oder Amazon EFS kopieren.	22. August 2019
<u>Support für die Verwendung von Virtual Private Cloud (VPC) -Endpunkten</u>	Sie können jetzt eine private Verbindung zwischen Ihrem Agenten und einem privaten Netzwerk herstellen AWS und Aufgaben in einem privaten Netzwerk ausführen. Dadurch wird die Sicherheit Ihrer Daten beim Kopieren über das Netzwerk erhöht.	5. August 2019
<u>Unterstützung von Endpunkten für den Federal Information Processing Standard (FIPS)</u>	Sie können nun FIPS-Endpunkte verwenden, um Agenten zu erstellen und Aufgaben auszuführen.	5. August 2019
<u>Neu AWS-Region</u>	AWS DataSync ist jetzt in der Region AWS GovCloud (US-West) verfügbar.	11. Juni 2019

[Support für Filterung](#)

Sie können jetzt Filter anwenden, um nur eine Teilmenge der Dateien in Ihrem Quellverzeichnis ins Zielverzeichnis zu übertragen.

22. Mai 2019

[Erste Version von AWS DataSync](#)

Allgemeine Veröffentlichung des AWS DataSync Dienstes.

26. November 2018

AWS Glossar

Die neueste AWS Terminologie finden Sie im [AWS Glossar](#) in der AWS-Glossar Referenz.

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.