Guida per l'utente

AWS DataSync

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS DataSync: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è AWS DataSync? 1
Casi d'uso 2
Vantaggi 3
Risorse aggiuntive 3
Come funziona 4
DataSync architettura di trasferimento 4
Trasferimento tra storage locale e AWS 4
Trasferimento tra AWS servizi di archiviazione 5
Trasferimento tra servizi AWS di storage e sistemi di storage in altri cloud 6
Concetti e terminologia 7
Agente 7
Ubicazione 8
Attività 8
Esecuzione dell'attività 8
Come DataSync trasferisce file, oggetti e directory 8
Come si DataSync prepara il trasferimento dei dati 8
Come DataSync trasferisce i tuoi dati 10
How DataSync verifica l'integrità dei dati 10
Come DataSync funziona con file aperti e bloccati 11
Opzioni di trasferimento ricorrenti 11
Nozioni di base 12
Iscriviti per un Account AWS 12
Crea un utente con accesso amministrativo 12
Autorizzazioni IAM richieste per l'utilizzo DataSync 14
AWS politiche gestite 14
Policy gestite dal cliente 14
Dove posso usare DataSync? 14
Come posso usare? DataSync 14
Quanto DataSync costerà? 15
Componenti open source utilizzati da DataSync 15
Ho bisogno di un agente? 15
Situazioni in cui è necessario un DataSync agente 15
Situazioni in cui non è necessario un agente DataSync 16
Utilizzo di più agenti DataSync 16

Passaggi successivi 17
Requisiti degli agenti 17
Requisiti dell'hypervisor 17
Requisiti degli agenti per DataSync i trasferimenti 18
Regione AWS Requisiti degli agenti per le partizioni 19
Requisiti di gestione degli agenti 19
Implementazione del tuo agente 19
Implementazione del tuo agente su VMware 20
Implementazione del tuo agente su KVM 20
Implementazione del tuo agente su Microsoft Hyper-V 21
Implementazione del tuo agente Amazon EC2 22
Implementazione del tuo agente su AWS Snowball Edge 28
Implementazione del tuo agente su AWS Outposts 28
Scelta di un endpoint di servizio per il vostro agente 28
Scelta di un endpoint di servizio pubblico 29
Scelta di un endpoint del servizio FIPS 29
Scelta di un endpoint di servizio VPC 30
Attivazione del tuo agente 32
Prerequisiti 32
Ottenere una chiave di attivazione 33
Attivazione del tuo agente 35
Passaggi successivi 37
Verifica delle connessioni di rete del tuo agente 38
Accesso alla console locale dell'agente 38
Verifica della connessione dell'agente al sistema di storage 39
Verifica della connessione del tuo agente al servizio DataSync 40
Passaggi successivi 40
Connessione della rete 41
1. Connessione di rete tra il sistema di storage e l'agente 41
2. Connessione di rete tra l'agente e DataSync il servizio 41
Connessione della rete di storage a AWS 42
Selezione di un endpoint del servizio 42
3. Connessione di rete tra il DataSync servizio e il servizio AWS di archiviazione 42
Collegamento in rete quando non è necessario un agente DataSync 43
Come e dove scorre DataSync il traffico attraverso la rete 43
Sicurezza di rete per DataSync 43

Requisiti di rete 43
IPv6 supporto 43
Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge 45
Requisiti di rete per i servizi AWS di storage 50
Requisiti di rete per gli endpoint di servizio pubblici o FIPS 51
Requisiti di rete per gli endpoint del servizio VPC 58
Interfacce di rete per il trasferimento di dati 61
Interfacce di rete per i trasferimenti con agenti 61
Interfacce di rete per trasferimenti senza agenti 62
Visualizzazione delle interfacce di rete 63
Esempi di architettura e routing con Direct Connect 64
Utilizzo di Direct Connect con un DataSync endpoint di servizio VPC 64
Utilizzo di Direct Connect con un DataSync endpoint di servizio pubblico o FIPS 67
Passaggi successivi 68
Configurazione del tuo agente per più persone NICs 68
Trasferimento dei dati 70
Dove posso trasferire i miei dati? 71
Trasferimenti supportati nello stesso Account AWS 71
Trasferimenti supportati tra Account AWS 73
Trasferimenti supportati nello stesso Regione AWS 74
Trasferimenti supportati tra Regioni AWS 74
Determinare se il trasferimento richiede un agente DataSync 75
Trasferimento da o verso lo storage locale 75
Configurazione dei trasferimenti con un file server NFS 76
Configurazione dei trasferimenti con un file server SMB 80
Configurazione dei trasferimenti con un cluster HDFS 91
Configurazione dei trasferimenti con un sistema di storage di oggetti 95
Trasferimento da o verso lo spazio di archiviazione AWS 100
Configurazione dei trasferimenti con Amazon S3 100
Configurazione dei trasferimenti con Amazon EFS 133
Configurazione dei trasferimenti con FSx per Windows File Server 143
Configurazione dei trasferimenti con for Lustre FSx 148
Configurazione dei trasferimenti con per OpenZFS FSx 150
Configurazione dei trasferimenti con for ONTAP FSx 153
Trasferimento da o verso un altro spazio di archiviazione cloud 161
Pianificazione dei trasferimenti da o verso sistemi di archiviazione cloud di terze parti 162

Configurazione dei trasferimenti con Google Cloud Storage 164
Configurazione dei trasferimenti con Microsoft Azure Blob Storage 173
Configurazione dei trasferimenti con Microsoft Azure Files 191
Configurazione dei trasferimenti con altri archivi di oggetti nel cloud 195
Trasferimento da o verso uno storage compatibile con S3 su Snowball Edge 202
Prerequisiti 202
Fornire DataSync l'accesso allo storage compatibile con S3 202
Creazione di un DataSync agente nell'ambiente di archiviazione locale 204
Configurazione della posizione di origine per il trasferimento 206
Configurazione della località di destinazione per il trasferimento 207
Configurazione delle impostazioni di trasferimento 207
Avvio del trasferimento 208
Limitazioni 208
Creazione di un'attività per il trasferimento dei dati 208
Creazione dell'attività 209
Stati delle attività 211
Partizionamento di set di dati di grandi dimensioni con più attività 212
Segmentazione dei dati trasferiti con più attività 212
Scelta di una modalità di operazione per il trasferimento 213
Scelta dei dati da trasferire 218
Verifica dell'integrità dei dati 257
Impostazione dei limiti di larghezza di banda 261
Pianificazione dell'attività 263
Etichettare le tue attività 267
Avvio di un'attività di trasferimento dei dati 270
Avvio della tua attività 271
Stati di esecuzione delle attività 272
Sapere quando l'attività è in coda 273
Annullamento dell'esecuzione dell'attività 274
Monitoraggio dei trasferimenti di dati 275
Comprensione dei contatori delle prestazioni di trasferimento dei dati 275
Monitoraggio dei trasferimenti di dati con metriche CloudWatch 294
CloudWatch metriche per DataSync 294
Monitoraggio dei trasferimenti di dati con report sulle attività 298
Casi d'uso 298
Riepilogano solo i rapporti sulle attività 299

Rapporti sulle attività standard 299
Esempi di report sulle attività 302
Limitazioni 306
Creazione dei report sulle attività 306
Visualizzazione delle relazioni sulle attività 316
Monitoraggio dei trasferimenti di dati con Logs CloudWatch 317
Consentire DataSync il caricamento dei log in un gruppo di CloudWatch log 317
Configurazione della registrazione per la tua attività DataSync 319
Visualizzazione dei registri delle DataSync attività 322
Registrazione con CloudTrail 323
Utilizzo delle DataSync informazioni in CloudTrail 324
Comprendere DataSync le voci dei file di registro 325
Monitoraggio con EventBridge 326
DataSync eventi di trasferimento 326
Monitoraggio con strumenti manuali 329
Monitoraggio del trasferimento tramite la DataSync console 329
Monitoraggio del trasferimento utilizzando il AWS CLI 329
Monitoraggio del trasferimento tramite l'`watch`utilità 331
Gestione delle risorse 332
Gestire il tuo DataSync agente 332
Verifica della connettività e delle risorse di sistema del tuo DataSync agente 332
Sostituzione del tuo agente DataSync 332
Pulizia DataSync delle risorse 332
Riutilizzo dell'infrastruttura di un DataSync agente 332
Gestire il proprio agente 332
Aggiornamenti del software dell'agente 333
Stati degli agenti 333
Risoluzione dei problemi relativi al tuo agente 334
Esecuzione della manutenzione del vostro agente 334
Accesso alla console locale dell'agente 334
Configurazione delle impostazioni DHCP, DNS e IP dell'agente 335
Verifica delle risorse di sistema del tuo agente 340
Sincronizzazione dell'ora sul tuo agente VMware 341
Esecuzione di comandi relativi alla manutenzione per l'agente 342
Sostituendo il tuo agente 344
Creazione di un nuovo agente 344

Aggiornamento della posizione con il nuovo agente 344
Passaggi successivi 349
Filtraggio DataSync delle risorse 350
Parametri per il filtraggio 350
Filtraggio per località 351
Filtraggio per attività 352
Pulizia DataSync delle risorse 353
Eliminazione di un agente DataSync 353
Riutilizzo dell'infrastruttura di un agente DataSync 354
Eliminazione di una posizione DataSync 355
Eliminazione di un'attività DataSync 355
Sicurezza 357
Protezione dei dati 358
Crittografia in transito 358
Crittografia a riposo 361
Riservatezza del traffico Internet 362
Gestione dell'identità e degli accessi 362
Gestione degli accessi 363
AWS politiche gestite 368
Policy gestite dal cliente 378
Uso di ruoli collegati ai servizi 381
Applicazione di tag alle risorse durante la creazione 385
Prevenzione del problema "confused deputy" tra servizi 387
Convalida della conformità 389
Resilienza 390
Sicurezza dell'infrastruttura 391
Protezione delle credenziali della posizione di archiviazione 391
Utilizzo di un segreto gestito dal servizio crittografato con una chiave predefinita 392
Utilizzo di un segreto gestito dal servizio crittografato con una chiave personalizzata AWS KMS 392
Usando un segreto che gestisci 394
Quote 397
Limiti del sistema di storage, dei file e degli oggetti 397
DataSync quote 397
Richiesta di un aumento della quota 403
Risoluzione dei problemi 404

Risoluzione dei problemi relativi agli agenti 404
Come posso connettermi alla console locale di un EC2 agente Amazon? 404
Cosa significa l'errore Failed to retrieve activation key dell'agente? 405
Non riesco ancora ad attivare un agente utilizzando un endpoint del servizio VPC 405
Cosa devo fare se il mio agente è offline? 405
Non so cosa stia succedendo con il mio agente. Qualcuno può aiutarmi? 406
Risoluzione dei problemi relativi alla posizione 407
La mia attività non è riuscita a causa di un errore NFS con autorizzazioni negate 407
La mia operazione non è riuscita a causa di un errore di montaggio NFS 408
La mia attività non è riuscita a causa di un errore di montaggio di Amazon EFS 408
La proprietà dei file non viene mantenuta con NFS Transfer 409
La mia attività non può accedere a una sede SMB che utilizza Kerberos 409
La mia operazione non è riuscita a causa di un input/output errore 410
Errore: `FsS3UnableToConnectToEndpoint` 411
Errore: `FsS3HeadBucketFailed` 412
L'operazione ha esito negativo con un `Unable to list Azure Blobs on the volume root` errore 412
Errore: `FsAzureBlobVolRootListBlobsFailed` 412
Errore: `SrcLocHitAccess` 413
Errore: `SyncTaskErrorLocationNotAdded` 413
Errore: `S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation` 413
L'operazione con posizione di origine S3 ha esito negativo con `HeadObject` o `GetObjectTagging` errore 413
Risoluzione dei problemi relativi alle attività 414
Errore: valore non valido SyncOption . Opzione: TransferMode,PreserveDeletedFiles, Valore: ALL, REMOVE. 414
L'esecuzione dell'operazione non riesce con un EniNotFounderrore 414
L'esecuzione dell'operazione non riesce con l'errore «Impossibile allocare la memoria» 415
L'operazione non riesce con `Input/Output error` il file system ONTAP 415
L'operazione non riesce con `Connection reset by host` o `Host is down` per il file system ONTAP 417
L'esecuzione dell'attività ha lo stato di avvio, ma sembra che non stia succedendo nulla 418
L'esecuzione dell'attività sembra bloccata nello stato di preparazione 418
L'esecuzione dell'attività si interrompe prima del termine del trasferimento 418

L'esecuzione dell'attività non riesce durante il trasferimento da un bucket di Google Cloud Storage ... 419
Vi sono discrepanze tra i timestamp di esecuzione dell'attività ... 419
L'esecuzione dell'attività fallisce con `NoMem` errori ... 420
`user metadata key`Errore nel trasferimento dell'oggetto Azure Blob Storage ... 420
C'è una `/.aws-datasync` cartella nella posizione di destinazione ... 420
Non è possibile trasferire collegamenti simbolici tra sedi utilizzando SMB ... 420
Errori nel report delle attività ... 421
Risoluzione dei problemi di verifica dei dati ... 422
Vi sono delle discrepanze tra i contenuti di un file ... 422
C'è una mancata corrispondenza tra i metadati SMB di un file ... 423
I file da trasferire non si trovano più nella posizione di origine ... 424
DataSync non è possibile verificare i dati di destinazione ... 425
DataSync non è in grado di leggere i metadati degli oggetti ... 426
C'è una mancata corrispondenza nei metadati definiti dal sistema di un oggetto ... 426
Comprensione della durata della verifica dei dati ... 428
Risoluzione dei problemi dei costi di storage S3 con DataSync ... 428
Tutorial ... 430
Trasferimento da locale a S3 tra account ... 430
Panoramica ... 430
Prerequisito: autorizzazioni richieste per l'account di origine ... 431
Prerequisito: autorizzazioni richieste per l'account di destinazione ... 433
Passaggio 1: nel tuo account di origine, crea un agente DataSync ... 434
Passaggio 2: nel tuo account di origine, crea un ruolo DataSync IAM per l'accesso al bucket di destinazione ... 434
Passaggio 3: nell'account di destinazione, aggiorna la policy sui bucket S3 ... 436
Passaggio 4: Nell'account di destinazione, disattivalo ACLs per il tuo bucket S3 ... 438
Passaggio 5: Nel tuo account di origine, crea una posizione di DataSync origine per lo storage locale ... 438
Passaggio 6: nel tuo account di origine, crea una posizione di DataSync destinazione per il tuo bucket S3 ... 439
Passaggio 7: Nel tuo account di origine, crea e avvia l'attività DataSync ... 440
Risorse correlate ... 440
Trasferimento tra bucket S3 tra account ... 441
Panoramica ... 442
Prerequisito: autorizzazioni richieste per l'account di origine ... 443

Prerequisito: autorizzazioni richieste per l'account di destinazione 446
Passaggio 1: nel tuo account di origine, crea un ruolo DataSync IAM per l'accesso al bucket di destinazione 446
Passaggio 2: nell'account di destinazione, aggiorna la policy sui bucket S3 448
Passaggio 3: nell'account di destinazione, disattivalo ACLs per il tuo bucket S3 450
Passaggio 4: Nel tuo account di origine, crea le tue DataSync sedi 450
Passaggio 5: Nel tuo account di origine, crea e avvia l'attività DataSync 452
Risoluzione dei problemi 454
Correlata: Trasferimenti tra account con bucket S3 utilizzando la crittografia lato server 452
Esecuzione di una migrazione su larga scala 455
Cos'è una migrazione di dati di grandi dimensioni? 455
Fasi chiave di una migrazione di dati di grandi dimensioni 455
Risorse aggiuntive 456
Fase 1: pianificazione della migrazione 456
Requisiti di raccolta 457
Esecuzione di un proof of concept 462
Stima delle tempistiche di migrazione 464
Fase 2: implementazione della migrazione 466
Accelerazione della migrazione con il partizionamento 467
Esecuzione DataSync delle attività 469
Monitoraggio dei trasferimenti 471
DataSync API 472
Azioni 472
CancelTaskExecution 475
CreateAgent 477
CreateLocationAzureBlob 482
CreateLocationEfs 489
CreateLocationFsxLustre 495
CreateLocationFsxOntap 499
CreateLocationFsxOpenZfs 504
CreateLocationFsxWindows 508
CreateLocationHdfs 513
CreateLocationNfs 520
CreateLocationObjectStorage 525
CreateLocationS3 533
CreateLocationSmb 540

CreateTask 548
DeleteAgent 558
DeleteLocation 560
DeleteTask 562
DescribeAgent 564
DescribeLocationAzureBlob 569
DescribeLocationEfs 574
DescribeLocationFsxLustre 580
DescribeLocationFsxOntap 583
DescribeLocationFsxOpenZfs 588
DescribeLocationFsxWindows 592
DescribeLocationHdfs 596
DescribeLocationNfs 601
DescribeLocationObjectStorage 605
DescribeLocationS3 610
DescribeLocationSmb 615
DescribeTask 621
DescribeTaskExecution 630
ListAgents 647
ListLocations 650
ListTagsForResource 653
ListTaskExecutions 656
ListTasks 659
StartTaskExecution 662
TagResource 669
UntagResource 672
UpdateAgent 674
UpdateLocationAzureBlob 676
UpdateLocationEfs 681
UpdateLocationFsxLustre 685
UpdateLocationFsxOntap 688
UpdateLocationFsxOpenZfs 691
UpdateLocationFsxWindows 694
UpdateLocationHdfs 698
UpdateLocationNfs 704
UpdateLocationObjectStorage 707

UpdateLocationS3 713
UpdateLocationSmb 717
UpdateTask 724
UpdateTaskExecution 730
Tipi di dati 732
AgentListEntry 735
AzureBlobSasConfiguration 737
CmkSecretConfig 738
CustomSecretConfig 740
Ec2Config 742
FilterRule 744
FsxProtocol 746
FsxProtocolNfs 747
FsxProtocolSmb 748
FsxUpdateProtocol 750
FsxUpdateProtocolSmb 752
HdfsNameNode 754
LocationFilter 755
LocationListEntry 757
ManagedSecretConfig 759
ManifestConfig 760
NfsMountOptions 762
OnPremConfig 764
Options 765
Platform 774
PrivateLinkConfig 775
QopConfiguration 777
ReportDestination 779
ReportDestinationS3 780
ReportOverride 782
ReportOverrides 783
ReportResult 785
S3Config 786
S3ManifestConfig 787
SmbMountOptions 789
SourceManifestConfig 791

TagListEntry 792
TaskExecutionFilesFailedDetail 793
TaskExecutionFilesListedDetail 795
TaskExecutionListEntry 797
TaskExecutionResultDetail 799
TaskFilter 802
TaskListEntry 804
TaskReportConfig 806
TaskSchedule 808
TaskScheduleDetails 810
Errori comuni 811
Parametri comuni 813
Cronologia dei documenti 816
AWS Glossario 830
..... dcccxxxi

Che cos'è AWS DataSync?

AWS DataSync è un servizio di trasferimento dati online che semplifica la migrazione dei dati e consente di trasferire in modo rapido, semplice e sicuro i dati di file o oggetti da, verso e tra AWS i servizi di archiviazione.

Trasferimenti di storage in locale

DataSync funziona con i seguenti sistemi di storage locali:

- Network File System (NFS)
- Server Message Block (SMB)
- File system distribuiti Hadoop (HDFS)
- Archiviazione di oggetti

AWS trasferimenti di archiviazione

DataSync funziona con i seguenti servizi AWS di archiviazione:

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Altri trasferimenti di spazio di archiviazione nel cloud

DataSync funziona con i seguenti servizi di archiviazione in altri cloud:

- 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

Trasferimenti di storage Edge

DataSync funziona con i seguenti servizi e dispositivi di edge storage:

- Storage compatibile con Amazon S3 su AWS Snowball Edge

Casi d'uso

Questi sono alcuni dei principali casi d'uso per DataSync:

- Migrazione dei dati: trasferimento rapido dei set di dati attivi attraverso la rete ai servizi di AWS storage. DataSync include la crittografia automatica e la convalida dell'integrità dei dati per garantire che i dati arrivino in modo sicuro, intatto e pronto all'uso.
- Archiviazione dei dati non aggiornati: sposta i dati archiviati nello storage locale direttamente in classi di storage a lungo termine durevoli e sicure come S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. In questo modo è possibile liberare capacità di archiviazione locale e spegnere i sistemi legacy.
- Replica dei dati: copia i dati in qualsiasi classe di storage Amazon S3, scegliendo la classe di storage più conveniente per le tue esigenze. Puoi anche inviare dati ad Amazon EFS, FSx per Windows File Server, FSx per Lustre o per OpenZFS FSx per un file system in standby.
- Trasferisci i dati per un'elaborazione tempestiva nel cloud: trasferisci i dati in entrata o in uscita per l'elaborazione. AWS Questo approccio velocizza i flussi di lavoro cloud ibridi critici in molti settori. Questi includono l'apprendimento automatico nel settore delle scienze della vita, la produzione di video nei media e nell'intrattenimento, l'analisi dei big data nei servizi finanziari e la ricerca sismica nel settore petrolifero e del gas.

Vantaggi

Utilizzando DataSync, puoi ottenere i seguenti vantaggi:

- Automatizza lo spostamento dei dati: DataSync semplifica il trasferimento dei dati sulla rete tra sistemi di storage e servizi. DataSync automatizza sia la gestione dei processi di trasferimento dei dati sia l'infrastruttura necessaria per trasferimenti di dati sicuri e ad alte prestazioni.
- Trasferimento sicuro dei dati: DataSync offre end-to-end sicurezza, inclusa la crittografia e la convalida dell'integrità dei dati, per garantire che i dati arrivino sicuri, intatti e pronti per l'uso. DataSync accede AWS allo storage tramite meccanismi di AWS sicurezza integrati, come AWS Identity and Access Management i ruoli (IAM). Supporta anche gli endpoint del cloud privato virtuale (VPC), offrendoti la possibilità di trasferire i dati senza attraversare la rete Internet pubblica e aumentando ulteriormente la sicurezza dei dati copiati online.
- Sposta i dati più velocemente: DataSync utilizza un protocollo di rete appositamente progettato e un'architettura parallela multithread per accelerare i trasferimenti. Questo approccio velocizza le migrazioni, i flussi di lavoro ricorrenti di elaborazione dei dati per l'analisi e l'apprendimento automatico e i processi di protezione dei dati.

Risorse aggiuntive

Consigliamo di leggere le sezioni seguenti:

- DataSync risorse: include blog, video e altri materiali di formazione
- AWS re:POST — Guarda le ultime discussioni in merito DataSync
- Prezzi di AWS DataSync

Come AWS DataSync funziona

Scopri i concetti chiave e la terminologia relativi ai AWS DataSync trasferimenti, incluso il modo in cui i dati vengono trasferiti da posizioni locali e cloud.

DataSync architettura di trasferimento

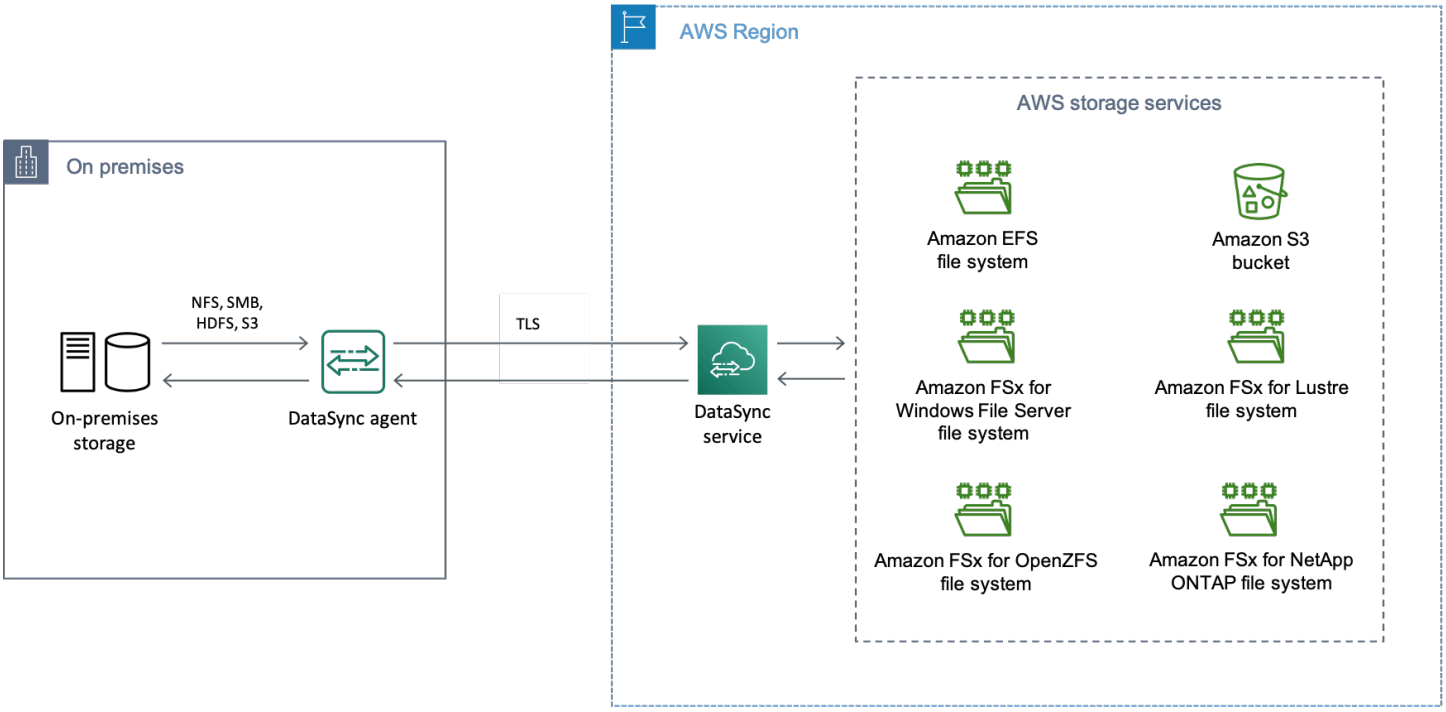
I seguenti diagrammi mostrano come e dove vengono DataSync comunemente trasferiti i dati di archiviazione. Per un elenco completo dei sistemi e dei servizi di storage DataSync supportati, vedere Con chi posso trasferire i miei dati AWS DataSync?

Argomenti

- Trasferimento tra storage locale e AWS
- Trasferimento tra AWS servizi di archiviazione
- Trasferimento tra servizi AWS di storage e sistemi di storage in altri cloud

Trasferimento tra storage locale e AWS

Il diagramma seguente mostra una panoramica di alto livello del DataSync trasferimento di file tra sistemi di storage locali autogestiti e. Servizi AWS

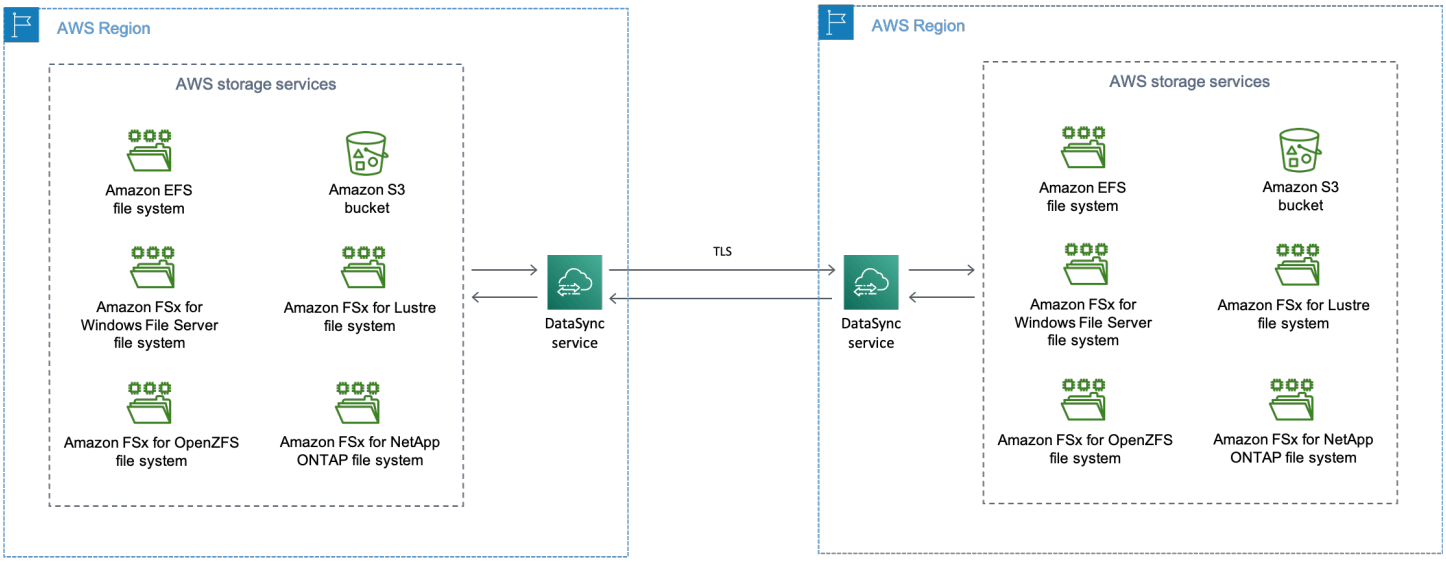


Il diagramma illustra un caso d'uso comune: DataSync

- Un DataSync agente che copia i dati da un sistema di storage locale.
- Trasferimento dei dati AWS, crittografati tramite Transport Layer Security (TLS).
- DataSync copia dei dati su un servizio di AWS archiviazione supportato.

Trasferimento tra AWS servizi di archiviazione

Il diagramma seguente mostra una panoramica di alto livello del DataSync trasferimento di file tra gli Servizi AWS stessi. Account AWS



Il diagramma illustra un caso d'uso comune: DataSync

- DataSync copia di dati da un servizio di archiviazione supportato AWS .
- Trasferimento di dati Regioni AWS, crittografati tramite TLS.
- DataSync copia dei dati su un servizio di AWS archiviazione supportato.

Durante il trasferimento tra servizi AWS di archiviazione (nello stesso Regione AWS o tra più servizi Regioni AWS), i dati rimangono nella AWS rete e non attraversano la rete Internet pubblica.

> **Important**
>
> Paghi per i dati trasferiti tra. Regioni AWS Questo viene fatturato come trasferimento di dati in uscita dalla regione di origine alla regione di destinazione. Per ulteriori informazioni, consulta Prezzi per il trasferimento dei dati.

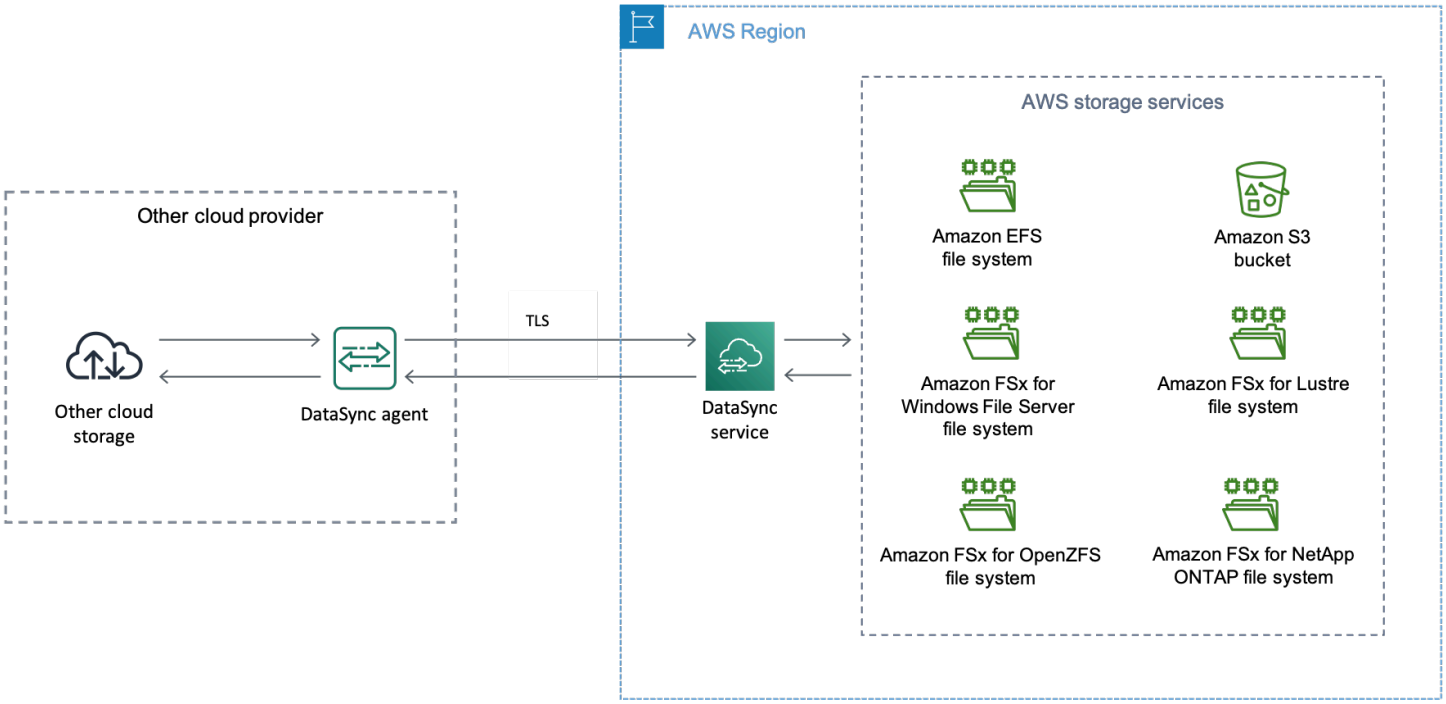
Trasferimento tra servizi AWS di storage e sistemi di storage in altri cloud

Con DataSync, puoi trasferire dati tra altri sistemi di archiviazione cloud e Servizi AWS. In questo contesto, i sistemi di archiviazione cloud possono includere:

- Sistemi di storage autogestiti, come un file server NFS nel tuo cloud privato virtuale (VPC) interno. AWS
- Sistemi o servizi di archiviazione ospitati da un altro provider di servizi cloud. Per ulteriori informazioni, consulta Trasferimento da o verso un altro spazio di archiviazione cloud con AWS DataSync.

DataSync può copiare dati da e verso altri cloud con o senza l'utilizzo di un agente. Per ulteriori informazioni su quando usare un agente, vedi Ho bisogno di un AWS DataSync agente? .

Il diagramma seguente mostra una panoramica di alto livello del DataSync trasferimento di dati tra i servizi di AWS archiviazione e un altro provider di servizi cloud.



Concetti e terminologia

Acquisisci familiarità con le funzionalità di trasferimento. DataSync

Argomenti

- Agente
- Ubicazione
- Attività
- Esecuzione dell'attività

Agente

Un agente è un'appliance di macchina virtuale (VM) che consente DataSync di leggere e scrivere sullo storage durante un trasferimento.

È possibile implementare un agente nel proprio ambiente di storage su VMware ESXi hypervisor KVM (Linux Kernel-based Virtual Machine) o Microsoft Hyper-V. Per lo storage in un cloud privato virtuale (VPC) in AWS, puoi implementare un agente come istanza Amazon. EC2

Per iniziare, consulta Ho bisogno di un AWS DataSync agente?

Ubicazione

Una posizione descrive da dove o verso cui stai copiando i dati. Ogni DataSync trasferimento (noto anche come operazione) ha una posizione di origine e una di destinazione. Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?

Attività

Un'attività descrive un DataSync trasferimento. Identifica una posizione di origine e una di destinazione insieme a dettagli su come copiare i dati tra tali posizioni. È inoltre possibile specificare in che modo un'attività gestisce i metadati, i file eliminati e le autorizzazioni.

Esecuzione dell'attività

L'esecuzione di un'attività è l'esecuzione individuale di un'operazione di DataSync trasferimento. L'esecuzione di un'attività prevede diverse fasi. Per ulteriori informazioni, consulta Stati di esecuzione delle attività.

Come DataSync trasferisce file, oggetti e directory

Durante l'esecuzione di un'attività, DataSync prepara, trasferisce e verifica i dati. DataSync Il modo in cui vengono eseguite queste azioni dipende da come si configurano le opzioni relative all' DataSync attività, ad esempio la modalità operazione. Le attività in modalità base preparano, trasferiscono e verificano i dati in sequenza, mentre le attività in modalità avanzata le eseguono in parallelo.

Argomenti

- Come si DataSync prepara il trasferimento dei dati
- Come DataSync trasferisce i tuoi dati
- How DataSync verifica l'integrità dei dati
- Come DataSync funziona con file aperti e bloccati
- Opzioni di trasferimento ricorrenti

Come si DataSync prepara il trasferimento dei dati

DataSync per impostazione predefinita, prepara il trasferimento esaminando le posizioni di origine e di destinazione per determinare cosa trasferire. Questo viene fatto scansionando il contenuto e i metadati di entrambe le località per identificare le differenze tra le due.

> **Note**
>
> Se configuri l'attività per trasferire tutti i dati, non è necessaria alcuna preparazione. All'inizio dell'attività, trasferisce DataSync immediatamente tutto dall'origine alla destinazione senza confrontare le posizioni.

DataSync La modalità di preparazione del trasferimento dipende anche dalla modalità di operazione:

Preparazione avanzata della modalità	Preparazione della modalità base
DataSync prepara gli oggetti così come si trovano nella posizione di origine. La preparazione continua per tutta l'esecuzione dell'attività fino a quando non ci sono più oggetti elencati all'origine.	La preparazione può richiedere solo pochi minuti, alcune ore o anche di più, a seconda del numero di file, oggetti o directory presenti in entrambe le ubicazioni e delle prestazioni dello storage.
A differenza della modalità Basic, DataSync è in grado di preparare un numero virtualmente illimitato di oggetti per ogni esecuzione di attività.	Gli articoli che vengono DataSync inventariati nell'origine e nella destinazione vengono conteggiati ai fini delle quote di attività. Queste quote non si basano sul numero di articoli che vengono DataSync trasferiti durante l'esecuzione di ogni attività.

DataSync potrebbe saltare alcuni file, oggetti e directory durante la preparazione. Le ragioni di ciò possono dipendere da diversi fattori, come la configurazione delle attività e le autorizzazioni del sistema di storage. Ecco alcuni esempi:

- Esiste un file nelle posizioni di origine e di destinazione. Il file nell'origine non è stato modificato dall'esecuzione dell'attività precedente. Poiché stai trasferendo solo dati che sono stati modificati, DataSync non trasferisce quel file la prossima volta che esegui l'operazione.
- Un oggetto che esiste in entrambe le posizioni cambia nella fonte. Quando esegui l'attività, DataSync salta questo oggetto nella destinazione perché l'attività non sovrascrive i dati nella destinazione.
- DataSync salta un oggetto nella posizione di origine che utilizza una classe di archiviazione e non viene ripristinato. È necessario ripristinare un oggetto archiviato per poterlo DataSync leggere.

- DataSync salta un file, un oggetto o una directory nella posizione di origine perché non può leggerlo. Se ciò accade e non è previsto, controlla le autorizzazioni di accesso dello spazio di archiviazione e assicurati che sia DataSync possibile leggere ciò che è stato ignorato.

Come DataSync trasferisce i tuoi dati

DataSync copia i dati (inclusi i metadati) dall'origine alla destinazione in base alle opzioni di attività. Ad esempio, puoi specificare quali metadati devono essere copiati, escludere determinati file e limitare la quantità di larghezza di banda DataSync utilizzata, tra le altre opzioni.

La modalità di DataSync trasferimento dei dati dipende anche dalla modalità di operazione:

Trasferimento in modalità avanzata	Trasferimento in modalità base
DataSync trasferisce ogni oggetto non appena viene preparato.	Una volta DataSync preparati tutti i dati, il trasferimento ha inizio.

DataSyncpotrebbe saltare alcuni elementi durante il trasferimento. Se si configura l'attività in modo da trasferire tutti i dati, ciò può accadere con un oggetto nella posizione di origine che utilizza una classe di archiviazione e non viene ripristinato.

How DataSync verifica l'integrità dei dati

DataSync esegue sempre controlli di integrità sui dati durante un trasferimento. Al termine di un trasferimento, DataSync può anche eseguire controlli aggiuntivi solo sui dati trasferiti o sull'intero set di dati in entrambe le posizioni. Per ulteriori informazioni, consulta Configurazione della modalità di AWS DataSync verifica dell'integrità dei dati.

Quando verifica l'integrità dei dati, DataSync calcola e confronta il checksum e i metadati dei file, degli oggetti o delle directory presenti nelle tue posizioni. Se DataSync rileva differenze tra le ubicazioni, la verifica fallisce e restituisce un errore. Ad esempio, potresti visualizzare errori come`Checksum failure`, `Metadata failure`o`Files were added`, `Files were removed`.

Il funzionamento della verifica dipende dalla modalità di operazione e dalla configurazione effettuata DataSync per verificare l'integrità dei dati al termine del trasferimento.

Verifica in modalità avanzata	Verifica in modalità base
DataSync verifica ogni oggetto man mano che viene trasferito a destinazione. Con la modalità avanzata, DataSync verifica solo i dati trasferiti.	Al termine del trasferimento, DataSync verifica l'integrità dei dati. A seconda di come configuri la verifica dei dati, questa operazione può richiedere molto tempo per set di dati di grandi dimensioni.

Come DataSync funziona con file aperti e bloccati

Tieni presente quanto segue quando cerchi di trasferire file aperti (in uso) o bloccati:

- In generale, DataSync può trasferire file aperti senza limitazioni.
- Se un file è aperto e viene scritto durante un trasferimento, DataSync è in grado di rilevare questo tipo di incongruenza durante la fase di verifica dell'attività di trasferimento. Per ottenere la versione più recente del file, è necessario eseguire nuovamente l'operazione.
- Se un file è bloccato e il server ne DataSync impedisce l'apertura, DataSync ignora il file durante il trasferimento e registra un errore.
- DataSync non è possibile bloccare o sbloccare file.

Opzioni di trasferimento ricorrenti

Oltre ai trasferimenti una tantum, DataSync può trasferire dati su base ricorrente. Alcune delle opzioni per queste situazioni includono:

- Pianificazione dell'esecuzione dell'attività.
- Trasferimento solo dei dati modificati dall'esecuzione dell'attività precedente.
- Eliminazione di dati nella posizione di destinazione che non sono più presenti nell'origine.

Guida introduttiva con AWS DataSync

Prima di iniziare AWS DataSync, devi registrarti Account AWS se non ne hai uno. Ti consigliamo inoltre di scoprire dove DataSync può essere utilizzato e quanto potrebbe costare trasferire i tuoi dati.

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Autorizzazioni IAM richieste per l'utilizzo DataSync

DataSync può trasferire i tuoi dati su un bucket Amazon S3, un file system Amazon EFS o una serie di altri AWS servizi di storage. Per portare i tuoi dati dove vuoi che vadano, hai bisogno delle giuste autorizzazioni IAM concesse alla tua identità. Ad esempio, il ruolo IAM che utilizzi DataSync richiede l'autorizzazione per utilizzare le operazioni Amazon S3 necessarie per trasferire dati in un bucket S3.

Puoi concedere queste autorizzazioni con le politiche IAM fornite da AWS o creando le tue politiche.

Indice

- AWS politiche gestite
- Policy gestite dal cliente

AWS politiche gestite

AWS fornisce le seguenti politiche gestite per casi DataSync d'uso comuni:

- `AWSDataSyncReadOnlyAccess`— Fornisce accesso in sola lettura a. DataSync
- `AWSDataSyncFullAccess`— Fornisce accesso completo DataSync e accesso minimo alle sue dipendenze.

Per ulteriori informazioni, consulta AWS politiche gestite per AWS DataSync.

Policy gestite dal cliente

È possibile creare policy IAM personalizzate da utilizzare con DataSync. Per ulteriori informazioni, consulta Politiche gestite dai clienti IAM per AWS DataSync.

Dove posso usare DataSync?

Per un elenco degli Regioni AWS endpoint che DataSync supportano, consulta AWS DataSync endpoint e quote in. Riferimenti generali di AWS

Come posso usare? DataSync

Esistono diversi modi di utilizzo DataSync:

- DataSync console, che fa parte di AWS Management Console.
- DataSync API o per configurare e gestire AWS CLIa livello di codice. DataSync
- AWS CloudFormationo Terraform per fornire le tue risorse. DataSync
- AWS SDKsper creare applicazioni che utilizzano DataSync.

Quanto DataSync costerà?

Nella pagina DataSync dei prezzi, crea una stima personalizzata utilizzando la quantità di dati che intendi trasferire.

Componenti open source utilizzati da DataSync

Per visualizzare i componenti open source utilizzati da DataSync, scarica il seguente link:

- datasync-open-source-components.zip

Ho bisogno di un AWS DataSync agente?

Per utilizzarlo AWS DataSync, potrebbe essere necessario un agente. Un agente è un'appliance di macchina virtuale (VM) che viene distribuita nell'ambiente di storage per il trasferimento dei dati.

La necessità o meno di un agente dipende da diversi fattori, tra cui il tipo di storage verso o da cui si sta effettuando il trasferimento, se si sta effettuando il trasferimento tra i due sistemi e tra Account AWS i quali Regioni AWS si sta effettuando il trasferimento. Prima di continuare a leggere, verifica che DataSync supporti il trasferimento che ti interessa.

Dopo aver stabilito che DataSync supporta lo scenario di trasferimento, consulta le seguenti informazioni per capire se hai bisogno di un agente.

Situazioni in cui è necessario un DataSync agente

La maggior parte delle situazioni che richiedono un DataSync agente riguardano lo storage gestito da te o da un altro provider di servizi cloud.

- Trasferimento tra i servizi AWS di archiviazione e l'archiviazione locale
- Trasferimento tra Amazon EFS o Amazon FSx e archiviazione in altri cloud
- Trasferimento da o verso l'edge storage

- Trasferimento tra alcuni servizi AWS di storage Account AWS (quando nessuno dei due servizi di storage è Amazon S3)

  Per ulteriori informazioni, consulta Trasferimenti supportati tra Account AWS.
- Trasferimento tra un negozio commerciale Regione AWS e uno AWS GovCloud (US) in cui l'origine e la destinazione sono Amazon EFS o Amazon FSx.

Situazioni in cui non è necessario un agente DataSync

Le situazioni che non richiedono un agente si applicano a prescindere dal fatto che il trasferimento avvenga nella stessa regione Regione AWS o in più regioni.

- Trasferimento tra servizi AWS di archiviazione all'interno della stessa Account AWS
- Trasferimento tra Amazon S3 e un AWS altro servizio di storage su Account AWS
- Trasferimento tra Amazon S3 e lo storage di oggetti in altri cloud
- Trasferimento tra uno spot commerciale Regione AWS e un altro AWS GovCloud (US) in cui l'origine o la destinazione è Amazon S3

Utilizzo di più agenti DataSync

Sebbene la maggior parte dei trasferimenti richieda un solo agente, l'utilizzo di più agenti può velocizzare i trasferimenti di set di dati di grandi dimensioni con milioni di file o oggetti. In queste situazioni, consigliamo di eseguire le attività di trasferimento in parallelo. Questo approccio distribuisce il carico di lavoro di trasferimento su più attività, ognuna delle quali utilizza il proprio agente. Inoltre, aiuta a ridurre il tempo necessario DataSync per preparare e trasferire i dati. Per ulteriori informazioni, consulta Partizionamento di set di dati di grandi dimensioni con più attività.

Un'altra opzione, specialmente se hai milioni di file di piccole dimensioni, consiste nell'utilizzare più agenti con una posizione di trasferimento. Ad esempio, puoi connettere fino a quattro agenti al servizio di file Network File System (NFS) locale. Questa opzione può velocizzare il trasferimento, anche se il tempo necessario DataSync per prepararlo non cambia.

Con entrambi gli approcci, tieni presente che questi possono aumentare le operazioni di I/O sullo storage e influire sulla larghezza di banda della rete. Per ulteriori informazioni sull'utilizzo di più agenti per i DataSync trasferimenti, consulta lo Storage Blog.AWS

Se stai pensando di utilizzare più agenti, ricorda quanto segue:

- L'utilizzo di più agenti con una sede non garantisce un'elevata disponibilità. Tutti gli agenti associati a una sede devono essere online prima di poter iniziare l'attività di trasferimento. Se uno degli agenti è offline, non puoi eseguire l'operazione.
- Se utilizzi un endpoint del servizio Virtual Private Cloud (VPC) per comunicare con il DataSync servizio, tutti gli agenti devono utilizzare lo stesso endpoint e la stessa sottorete.

Passaggi successivi

- Se hai bisogno di un agente, consulta i requisiti dell'agente per capire cosa è utile per il tuo ambiente di storage.
- Se non hai bisogno di un agente per il trasferimento, puoi iniziare a configurare il trasferimento.

Requisiti per gli agenti AWS DataSync

Prima di implementare un AWS DataSync agente nel tuo ambiente di storage, assicurati di comprendere i requisiti dell'agente, dell'hypervisor e delle risorse.

Requisiti dell'hypervisor

È possibile eseguire un DataSync agente sui seguenti hypervisor:

- VMware ESXi (versione 6.5, 6.7, 7.0 o 8.0): VMware ESXi è disponibile sul sito Web di Broadcom. È inoltre necessario un client VMware vSphere per connettersi all'host.
- Macchina virtuale basata su kernel Linux (KVM): una tecnologia di virtualizzazione gratuita e open source. KVM è incluso nelle versioni Linux 2.6.20 e successive. DataSync è testato e supportato per le distribuzioni CentOS/RHEL 7 e 8, Ubuntu 16.04 LTS e Ubuntu 18.04 LTS. Altre distribuzioni Linux moderne potrebbero funzionare, ma la funzionalità o le prestazioni non sono garantite. È necessario abilitare la virtualizzazione con accelerazione hardware sull'host KVM per distribuire l'agente. DataSync

  Consigliamo questa opzione se disponi già di un ambiente KVM attivo e funzionante e conosci già il funzionamento di KVM.

  L'esecuzione di KVM su Amazon EC2 non è supportata e non può essere utilizzata per gli DataSync agenti.
- Microsoft Hyper-V (versione 2012 R2, 2016 o 2019): per questa configurazione, è necessario un Microsoft Hyper-V Manager su un computer client Microsoft Windows per connettersi all'host.

L' DataSync agente è una macchina virtuale (VM) di prima generazione. Per ulteriori informazioni sulle differenze tra la prima e la seconda generazione VMs, vedi Devo creare una macchina virtuale di prima o seconda generazione in Hyper-V?

- Amazon EC2: DataSync fornisce un'Amazon Machine Image (AMI) che contiene l' DataSync immagine. Per i tipi di istanza consigliati, consulta Requisiti delle EC2 istanze Amazon.

Requisiti degli agenti per DataSync i trasferimenti

Per DataSync i trasferimenti, l'agente deve soddisfare i seguenti requisiti di risorse.

> **Important**
>
> Tieni presente che i requisiti dell'agente per lavorare con un massimo di 20 milioni di file, oggetti o directory sono linee guida generali. Il tuo agente potrebbe aver bisogno di più risorse a causa di altri fattori, come il numero di directory e le dimensioni dei metadati degli oggetti. Ad esempio, l'istanza m5.2xlarge per un EC2 agente Amazon potrebbe non essere ancora sufficiente per un trasferimento di meno di 20 milioni di file.

Indice

- Requisiti delle macchine virtuali
- Requisiti delle EC2 istanze Amazon

Requisiti delle macchine virtuali

Quando si distribuisce un DataSync agente che non si trova su un' EC2 istanza Amazon, la macchina virtuale dell'agente richiede le seguenti risorse:

- Processori virtuali: quattro processori virtuali assegnati alla macchina virtuale.
- Spazio su disco: 80 GB di spazio su disco per l'installazione dell'immagine della VM e dei dati di sistema.
- RAM: a seconda dello scenario di trasferimento, è necessaria la seguente quantità di memoria:
  - 32 GB di RAM assegnati alla macchina virtuale per l'esecuzione di attività con un massimo di 20 milioni di file, oggetti o directory.

- 64 GB di RAM assegnati alla macchina virtuale per l'esecuzione di attività con più di 20 milioni di file, oggetti o directory.

Requisiti delle EC2 istanze Amazon

Quando si distribuisce un DataSync agente su un' EC2 istanza Amazon, la dimensione dell'istanza deve essere almeno 2 volte più grande.

Ti consigliamo di utilizzare una delle seguenti dimensioni di istanza:

- m5.2xlarge: per l'esecuzione di attività con un massimo di 20 milioni di file, oggetti o directory.
- m5.4xlarge: per le esecuzioni di attività che utilizzano più di 20 milioni di file, oggetti o directory.

Regione AWS Requisiti degli agenti per le partizioni

DataSync le immagini degli agenti sono associate a Regione AWS partizioni specifiche. Ad esempio, per impostazione predefinita non è possibile scaricare un agente in uno spot pubblicitario Regione AWS e poi attivarlo in un AWS GovCloud (US) Region.

Requisiti di gestione degli agenti

Una volta attivato il tuo DataSync agente, lo AWS gestisce per te. Per ulteriori informazioni, consulta Gestire il tuo AWS DataSync agente.

Implementazione del tuo agente AWS DataSync

Quando si crea un AWS DataSync agente, il primo passo è quello di implementarlo nel proprio ambiente di storage. È possibile distribuire un agente come macchina virtuale (VM) su VMware ESXi hypervisor KVM (Linux Kernel-based Virtual Machine) e Microsoft Hyper-V. Puoi anche implementare un agente come EC2 istanza Amazon in un cloud privato virtuale (VPC) interno. AWS

> **Tip**
>
> Prima di iniziare, conferma se hai bisogno di un DataSync agente.

Implementazione del tuo agente su VMware

Puoi scaricare un agente dalla DataSync console e distribuirlo nel tuo VMware ambiente.

Prima di iniziare: assicurati che il tuo ambiente di storage sia in grado di supportare un DataSync agente. Per ulteriori informazioni, consulta Requisiti delle macchine virtuali.

Per distribuire un agente su VMware

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Agenti, quindi scegli Crea agente.
3. Per Hypervisor, scegli VMWare ESXi, quindi scegli Scarica l'immagine.

   L'agente scarica un `.zip` file che contiene un file di `.ova` immagine.
4. Per ridurre al minimo la latenza di rete, è necessario installare l'agente il più vicino possibile al sistema di storage a cui DataSync deve accedere (se possibile la stessa rete locale). Per ulteriori informazioni, consulta Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge.

   Se necessario, consultate la documentazione dell'hypervisor su come distribuire un file in un `.ova` host. VMware
5. Accendi l'hypervisor, accedi alla macchina virtuale dell'agente e ottieni l'indirizzo IP dell'agente. perché servirà per attivarlo.

   Le credenziali predefinite della macchina virtuale dell'agente sono login e password. **`admin password`** Se necessario, modificare la password tramite la console locale della macchina virtuale.

Passaggio successivo: Scelta di un endpoint di servizio per il tuo agente AWS DataSync

Implementazione del tuo agente su KVM

Puoi scaricare un agente dalla DataSync console e distribuirlo nel tuo ambiente KVM.

Prima di iniziare: assicurati che il tuo ambiente di storage sia in grado di supportare un agente. DataSync Per ulteriori informazioni, consulta Requisiti delle macchine virtuali.

Per distribuire un agente su KVM

1. Apri la console all' AWS DataSync indirizzo. https://console.aws.amazon.com/datasync/

2. Nel riquadro di navigazione a sinistra, scegli Agenti, quindi scegli Crea agente.
3. Per Hypervisor, scegli Kernel-based Virtual Machine (KVM), quindi scegli Scarica l'immagine.

   L'agente scarica un file che contiene un `.zip` file di immagine. `.qcow2`
4. Per ridurre al minimo la latenza di rete, è necessario installare l'agente il più vicino possibile al sistema di storage a cui DataSync deve accedere (se possibile la stessa rete locale). Per ulteriori informazioni, consulta Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge.
5. Esegui il comando seguente per installare l'`.qcow2`immagine.

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

   Per informazioni su come gestire questa macchina virtuale e il tuo host KVM, consulta la documentazione dell'hypervisor.
6. Attivare l'hypervisor, accedere alla VM e recuperare l'indirizzo IP dell'agente, perché servirà per attivarlo.

   Le credenziali predefinite dell'agente VM sono login e password. **`admin`** **`password`** Se necessario, modificare la password tramite la console locale della macchina virtuale.

Passaggio successivo: Scelta di un endpoint di servizio per il tuo agente AWS DataSync

Implementazione del tuo agente su Microsoft Hyper-V

È possibile scaricare un agente dalla DataSync console e distribuirlo nell'ambiente Microsoft Hyper-V.

Prima di iniziare: assicurati che il tuo ambiente di storage sia in grado di supportare un agente. DataSync Per ulteriori informazioni, consulta Requisiti delle macchine virtuali.

Per distribuire un agente su Hyper-V

1. Apri la console all' AWS DataSync indirizzo. https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione a sinistra, scegli Agenti, quindi scegli Crea agente.
3. Per Hypervisor, scegli Microsoft Hyper-V, quindi scegli Scarica l'immagine.

   L'agente viene scaricato in un `.zip` file che contiene un file di immagine. `.vhdx`
4. Per ridurre al minimo la latenza di rete, è necessario installare l'agente il più vicino possibile al sistema di storage a cui DataSync deve accedere (se possibile la stessa rete locale). Per ulteriori informazioni, consulta Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge.

   Se necessario, consulta la documentazione del tuo hypervisor su come distribuire un `.vhdx` file in un host Hyper-V.

   > **Warning**
   >
   > Potresti notare prestazioni di rete scadenti se abiliti la coda di macchine virtuali (VMQ) su un host Hyper-V che utilizza una scheda di rete Broadcom. Per informazioni su una soluzione alternativa, consulta la documentazione Microsoft.
5. Attivare l'hypervisor, accedere alla VM e recuperare l'indirizzo IP dell'agente, perché servirà per attivarlo.

   Le credenziali predefinite dell'agente VM sono login **`admin`** e password. **`password`** Se necessario, modificare la password tramite la console locale della macchina virtuale.

Passaggio successivo: Scelta di un endpoint di servizio per il tuo agente AWS DataSync

Implementazione del tuo agente Amazon EC2

Puoi implementare un DataSync agente come EC2 istanza Amazon durante il trasferimento di dati tra:

- Un sistema di archiviazione cloud autogestito (ad esempio, un file server NFS AWS) e un servizio di archiviazione. AWS
- Un provider di archiviazione cloud (come Microsoft Azure Blob Storage o Google Cloud Storage) e un servizio di AWS archiviazione.

- Un bucket S3 in uno spot pubblicitario Regione AWS e un bucket S3 in un. AWS GovCloud (US) Region
- Amazon S3 attivo AWS Outposts e un servizio di AWS storage.

> **Warning**
>
> Non consigliamo di utilizzare un EC2 agente Amazon con storage locale a causa della maggiore latenza di rete. Invece, distribuisci l'agente come macchina virtuale KVM o Hyper-V nel tuo data center il più vicino possibile allo storage locale. VMware

EC2 Implementazione del tuo agente

Per scegliere l'agente AMI per te Regione AWS

1. Apri un terminale e copia il seguente AWS CLI comando per ottenere l'ID DataSync Amazon Machine Image (AMI) più recente per la regione in cui desideri distribuire il tuo EC2 agente Amazon.

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

2. Esegui il comando . Nell'output, prendi nota della `"Value"` proprietà con l'ID DataSync AMI.

   Example Esempio di comando e output

   ```
   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"
       }
   }
   ```

Per distribuire il tuo agente Amazon EC2

> **Tip**
>
> Per evitare addebiti per il trasferimento tra zone di disponibilità, implementa il tuo agente in modo che non richieda traffico di rete tra le zone di disponibilità. (Per ulteriori informazioni sui prezzi di trasferimento dati per tutti Regioni AWS, consulta i prezzi di Amazon EC2 Data Transfer.)
> Ad esempio, distribuisci il tuo agente nella zona di disponibilità in cui si trova il tuo sistema di archiviazione cloud autogestito.

1. Copia il seguente URL:

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

   - Sostituiscilo *agent-region* con la regione in cui desideri distribuire l'agente.
   - Sostituisci *ami-id* con l'ID DataSync AMI che hai ottenuto.
2. Incollare l'URL in un browser.

   La pagina di avvio dell' EC2 istanza Amazon AWS Management Console viene visualizzata nei display.
3. Per Tipo di istanza, scegli una delle EC2 istanze Amazon consigliate per DataSync.
4. Per Coppia di chiavi, scegli una coppia di chiavi esistente o creane una nuova.
5. Per Impostazioni di rete, scegliete Modifica, quindi effettuate le seguenti operazioni:

   a. Per VPC, scegli un VPC in cui desideri implementare il tuo agente.

   b. Per l'assegnazione automatica dell'IP pubblico, scegli se desideri che il tuo agente sia accessibile dalla rete Internet pubblica.

      In un secondo momento utilizzerai l'indirizzo IP pubblico o privato dell'istanza per attivare l'agente.

   c. Per Firewall (gruppi di sicurezza), crea o seleziona un gruppo di sicurezza che esegua le seguenti operazioni:

- Se necessario, consente il traffico in entrata verso l' EC2istanza Amazon sulla porta 80 (HTTP). Alcune opzioni per ottenere una chiave di attivazione dell'agente richiedono questa connessione.
- Consente il traffico in entrata e in uscita tra l' EC2 istanza Amazon e il sistema di storage verso cui trasferisci o da cui trasferisci i dati. Per ulteriori informazioni, consulta Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge.

> **Note**
>
> Esistono porte aggiuntive da configurare a seconda del tipo di endpoint di servizio utilizzato dall'agente.

6. (Consigliato) Per aumentare le prestazioni durante il trasferimento da un file system basato sul cloud, espandi Advanced details e scegli un valore del gruppo Placement in cui si trova lo storage.
7. Scegli Launch instance per avviare la tua EC2 istanza Amazon.
8. Una volta che lo stato dell'istanza è in esecuzione, scegli l'istanza.
9. Se hai configurato l'istanza per essere accessibile dalla rete Internet pubblica, prendi nota dell'indirizzo IP pubblico dell'istanza. In caso contrario, prendi nota dell'indirizzo IP privato.

   Hai bisogno di questo indirizzo IP per attivare il tuo agente.

Esempi: Implementazione dell' EC2agente in un Regione AWS

Le seguenti indicazioni possono essere utili negli scenari più comuni se si distribuisce un DataSync agente in un. Regione AWS

Argomenti

- Implementazione del tuo agente per i trasferimenti tra cloud storage e AWS servizi di archiviazione
- Implementazione del tuo agente per i trasferimenti tra Amazon S3 AWS e i file system

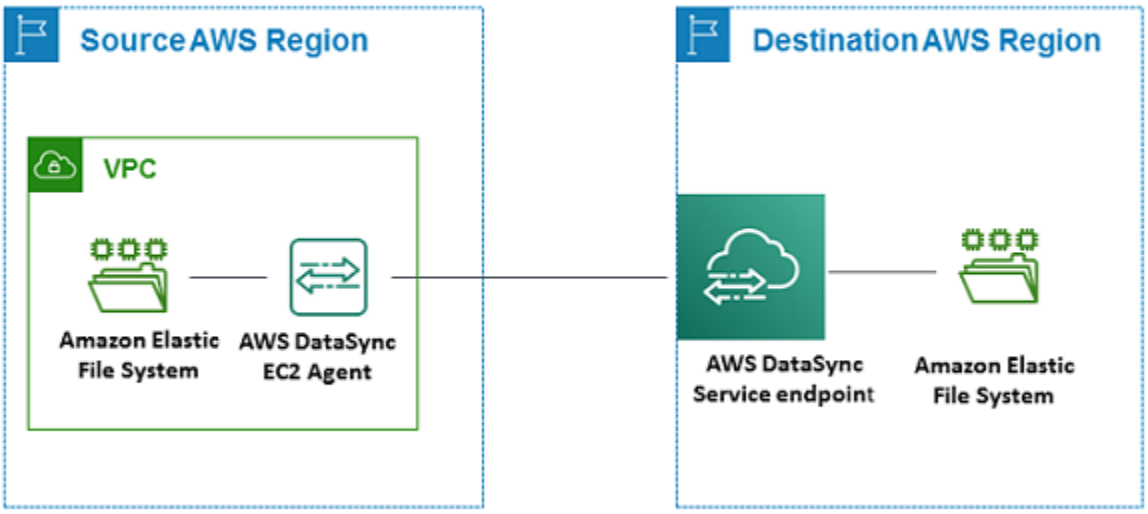
Implementazione del tuo agente per i trasferimenti tra cloud storage e AWS servizi di archiviazione

Per trasferire dati tra Account AWS o tra sistemi di archiviazione cloud, l' DataSync agente deve trovarsi nello stesso Regione AWS e Account AWS dove risiede il file system di origine. Questo tipo di trasferimento include quanto segue:

- Trasferimenti tra Amazon EFS o Amazon FSx verso uno AWS storage diverso Account AWS.
- Trasferimenti da file system autogestiti a servizi AWS di storage.

> **Important**
>
> Implementa il tuo agente in modo che non richieda traffico di rete tra le zone di disponibilità (per evitare addebiti per tale traffico).
>
> - Per accedere al tuo file system Amazon EFS o FSx per Windows File Server, distribuisci l'agente in una zona di disponibilità con una destinazione di montaggio sul tuo file system.
> - Per i file system autogestiti, distribuisci l'agente nella zona di disponibilità in cui risiede il file system.
>
> Per ulteriori informazioni sui prezzi di trasferimento dati per tutti Regioni AWS, consulta i prezzi di Amazon EC2 On-Demand.

Ad esempio, il diagramma seguente mostra una vista di alto livello dell' DataSync architettura per il trasferimento di dati da Network File System (NFS) nel cloud a NFS in-cloud o Amazon S3.

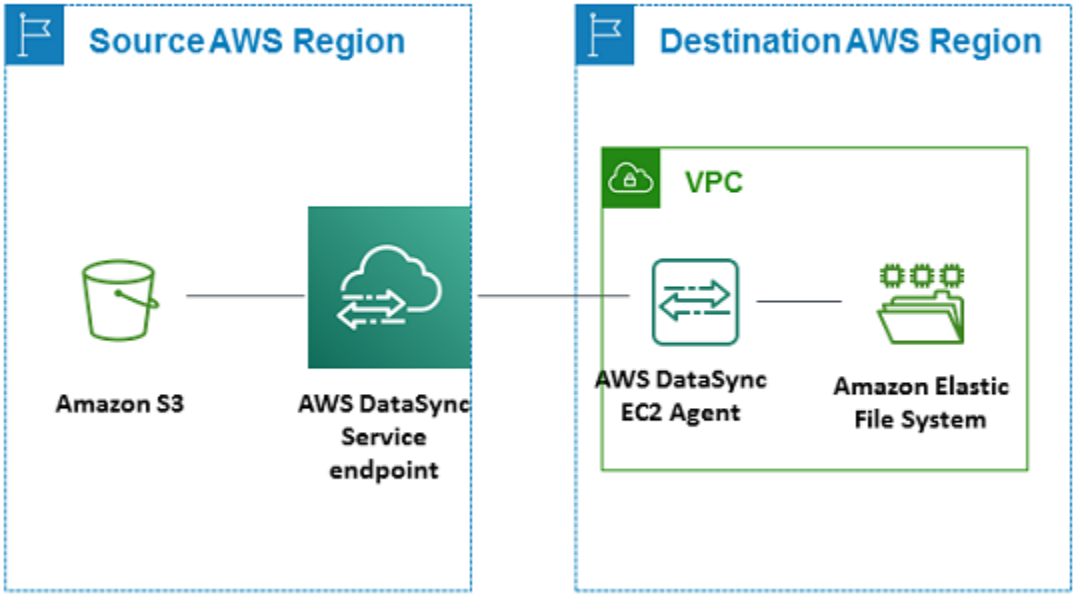


Tieni presente quanto segue quando effettui il trasferimento tra AWS servizi di storage su: Account AWS

- Quando effettui il trasferimento tra file system Amazon EFS o FSx file system Amazon utilizzando il protocollo NFS, configura il file system di origine come posizione NFS.
- Quando effettui il trasferimento tra FSx file system Amazon utilizzando il protocollo SMB, configura il file system di origine come posizione SMB.

Implementazione del tuo agente per i trasferimenti tra Amazon S3 AWS e i file system

Il diagramma seguente fornisce una visione di alto livello dell' DataSyncarchitettura per il trasferimento di dati da Amazon S3 a un AWS file system, come Amazon EFS o Amazon. FSx Puoi utilizzare questa architettura per trasferire dati da uno Account AWS all'altro o trasferire dati da Amazon S3 a un file system in-cloud autogestito.



Implementazione del tuo agente su AWS Snowball Edge

Per ulteriori informazioni e istruzioni, consulta lo Creazione di un DataSync agente nell'ambiente di archiviazione locale storage compatibile con Amazon S3.

Implementazione del tuo agente su AWS Outposts

Puoi avviare un' EC2 istanza DataSync Amazon sul tuo Outpost. Per ulteriori informazioni sul lancio di un'AMI su AWS Outposts, consulta Launch an istance on Outpost nella Guida per l'AWS Outposts utente.

Quando si utilizza DataSync per accedere ad Amazon S3 su Outposts, è necessario avviare l'agente in un VPC autorizzato ad accedere al punto di accesso Amazon S3 e attivare l'agente nella regione principale dell'Outpost. L'agente deve inoltre essere in grado di effettuare il routing verso l'endpoint Amazon S3 on Outposts per il bucket. Per ulteriori informazioni su come lavorare con Amazon S3 sugli endpoint Outposts, consulta Working with Amazon S3 on Outposts nella Amazon S3 User Guide.

Scelta di un endpoint di servizio per il tuo agente AWS DataSync

Un endpoint del servizio è il modo in cui AWS DataSync l'agente comunica con il servizio. DataSync DataSync supporta i seguenti tipi di endpoint di servizio:

- Endpoint di servizio pubblico: i dati vengono inviati tramite la rete Internet pubblica.
- Endpoint del servizio Federal Information Processing Standard (FIPS): i dati vengono inviati sulla rete Internet pubblica utilizzando processi conformi allo standard FIPS.
- Endpoint del servizio Virtual Private Cloud (VPC): i dati vengono inviati tramite il tuo VPC anziché tramite la rete Internet pubblica, aumentando la sicurezza dei dati trasferiti.

È necessario un endpoint di servizio per attivare l'agente. Quando scegli un endpoint di servizio, ricorda quanto segue:

- Un agente può utilizzare solo un tipo di endpoint. Se devi trasferire dati utilizzando diversi tipi di endpoint, crea un agente per ogni tipo.
- Il modo in cui si connette la rete di storage AWS determina quali endpoint di servizio è possibile utilizzare.

Scelta di un endpoint di servizio pubblico

Se si utilizza un endpoint di servizio pubblico, tutte le comunicazioni tra l' DataSync agente e il DataSync servizio avvengono sulla rete Internet pubblica.

1. Determina l'endpoint del servizio DataSync pubblico che desideri utilizzare.
2. Configura la tua rete per consentire il traffico necessario per l'utilizzo degli endpoint del servizio DataSync pubblico.

Fase successiva: Attivazione del tuo agente AWS DataSync

Scelta di un endpoint del servizio FIPS

DataSync fornisce alcuni endpoint di servizio conformi allo standard FIPS. Per ulteriori informazioni, vedere Endpoint FIPS in. Riferimenti generali di AWS

1. Determina l'endpoint del servizio DataSync FIPS che desideri utilizzare.
2. Configura la tua rete per consentire il traffico necessario per l'utilizzo degli endpoint del servizio DataSync FIPS.

Fase successiva: Attivazione del tuo agente AWS DataSync

Scelta di un endpoint di servizio VPC

Se utilizzi un endpoint del servizio VPC, i tuoi dati non vengono trasferiti sulla rete Internet pubblica. DataSync trasferisce invece i dati tramite un VPC basato sul servizio Amazon VPC.

Indice

- Come DataSync gli agenti lavorano con gli endpoint dei servizi VPC
- DataSync limitazioni con VPCs
- Creazione di un endpoint di servizio VPC per DataSync

Come DataSync gli agenti lavorano con gli endpoint dei servizi VPC

Gli endpoint del servizio VPC sono forniti da. AWS PrivateLink Questi tipi di endpoint ti consentono di connetterti privatamente con supporto Servizi AWS al tuo VPC. Quando utilizzi un endpoint del servizio VPC con DataSync, tutte le comunicazioni tra l' DataSync agente e il DataSync servizio rimangono nel tuo VPC.

Gli endpoint del servizio VPC (insieme alle interfacce di rete DataSync create per il traffico di trasferimento dati) sono indirizzi IP privati accessibili solo dall'interno del VPC. Per ulteriori informazioni, consulta Connessione della rete per AWS DataSync i trasferimenti.

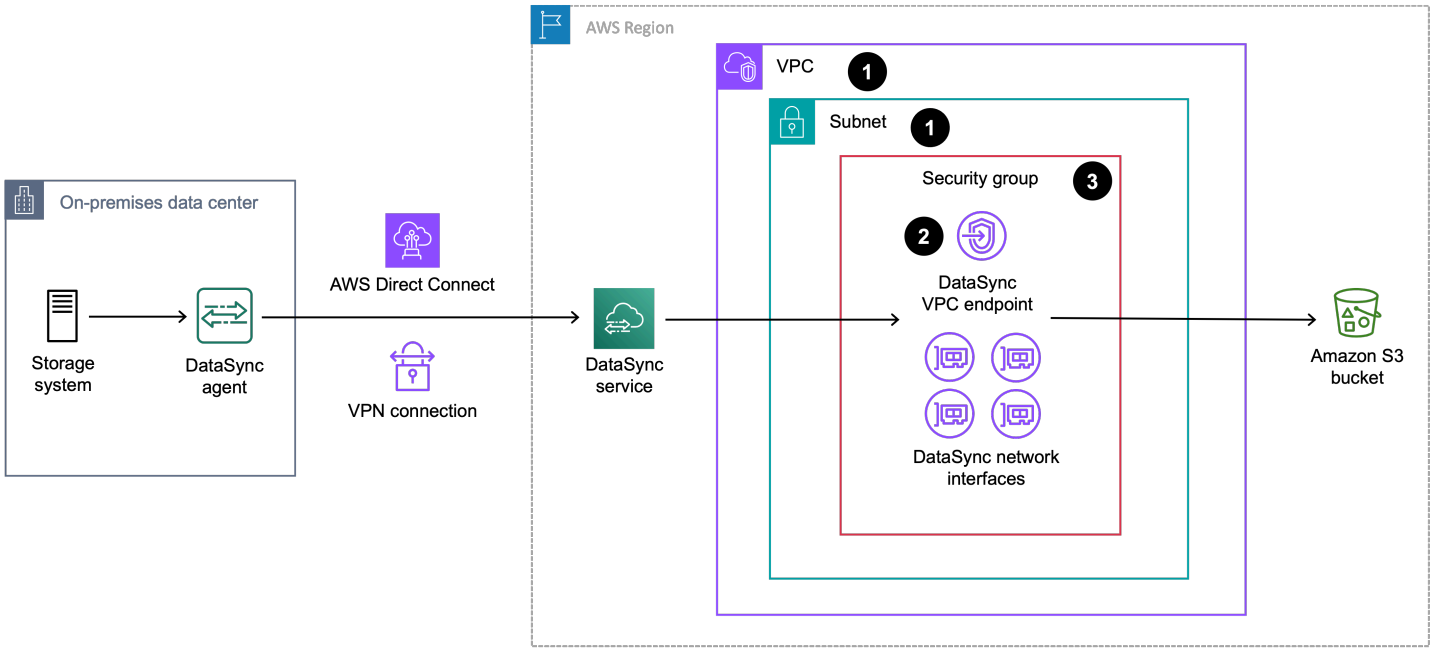
DataSync limitazioni con VPCs

- VPCs che usi con DataSync deve avere una locazione predefinita. VPCs con locazione dedicata non sono supportati.
- DataSync non supporta la condivisione VPCs.

Creazione di un endpoint di servizio VPC per DataSync

Crei un endpoint di servizio VPC per DataSync un VPC che gestisci. L'endpoint di servizio, il VPC DataSync e l'agente devono appartenere allo stesso. Account AWS

Il diagramma seguente mostra un esempio di DataSync utilizzo di un endpoint del servizio VPC per il trasferimento da un sistema di storage locale a un bucket Amazon S3. I callout numerati corrispondono ai passaggi per creare un endpoint di servizio VPC.



Per creare un endpoint del servizio VPC per DataSync

1. Crea o determina un VPC e una sottorete in cui desideri creare l'endpoint del servizio VPC.

   Se stai trasferendo da o verso uno storage esterno AWS, il VPC dovrebbe estendersi a quell'ambiente di storage (ad esempio, l'ambiente di storage potrebbe essere un data center in cui si trova il file server NFS locale). È possibile farlo utilizzando le regole di routing over o la VPN. AWS Direct Connect
2. Crea un endpoint del servizio DataSync VPC effettuando le seguenti operazioni:

   a. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

   b. Nel riquadro di navigazione a sinistra, scegli Endpoints, quindi scegli Crea endpoint.

   c. Per Service category (Categoria servizio), scegli Servizi AWS.

   d. Per Servizi, cerca **`datasync`** e scegli l'endpoint per la regione in cui ti trovi (ad esempio,). `com.amazonaws.us-east-1.datasync`

   e. Per VPC, scegli il VPC in cui desideri creare l'endpoint del servizio VPC.

   f. Espandi Impostazioni aggiuntive e deseleziona la casella di controllo Abilita nome DNS privato per disabilitare questa impostazione.

      Ti consigliamo di disabilitare questa impostazione nel caso in cui ci siano agenti nello stesso VPC che devono utilizzare un endpoint di servizio pubblico. Un agente non può raggiungere un endpoint di servizio pubblico sulla rete quando questa impostazione è abilitata.

g. Per Subnet, scegli la sottorete in cui desideri creare l'endpoint del servizio VPC. Prendi nota dell'ARN della sottorete (è necessario quando si attiva l'agente).

h. Seleziona Crea endpoint. Prendi nota dell'ID dell'endpoint (ne hai bisogno per attivare il tuo agente).

3. Nel tuo VPC, configura un gruppo di sicurezza che consenta il traffico necessario per l'utilizzo degli endpoint del servizio DataSync VPC. Prendi nota dell'ARN del gruppo di sicurezza (ne hai bisogno quando attivi il tuo agente).

   Il gruppo di sicurezza deve consentire all'agente di connettersi con gli indirizzi IP privati dell'endpoint del servizio VPC e delle interfacce di rete (che vengono create quando si crea l'attività).

Fase successiva: Attivazione del tuo agente AWS DataSync

Attivazione del tuo agente AWS DataSync

Per completare la creazione del tuo AWS DataSync agente, devi attivarlo. Questo passaggio associa l'agente al tuo Account AWS.

> **Note**
>
> Non puoi attivare un agente in più di un Account AWS agente Regione AWS alla volta.

Prerequisiti

Per attivare il tuo DataSync agente, assicurati di disporre delle seguenti informazioni:

- L'endpoint del DataSync servizio con cui stai attivando il tuo agente.

  Se utilizzi un endpoint di servizio VPC, hai bisogno di questi dettagli:

  - L'ID dell'endpoint del servizio VPC.
  - La sottorete in cui si trova l'endpoint del servizio VPC.
  - Il gruppo di sicurezza che consente il traffico richiesto per l'utilizzo degli endpoint del servizio DataSync VPC.
- L'indirizzo IP o il nome di dominio del tuo agente.

Il modo in cui lo trovi dipende dal tipo di agente che distribuisci. Ad esempio, se il tuo agente è un' EC2 istanza Amazon, puoi trovare il suo indirizzo IP accedendo alla pagina dell'istanza sulla EC2 console Amazon.

Ottenere una chiave di attivazione

È possibile ottenere una chiave di attivazione per l' DataSync agente distribuito in diversi modi. Alcune opzioni richiedono l'accesso all'agente sulla porta 80 (HTTP). Se utilizzi una di queste opzioni, DataSync chiude la porta una volta attivato l'agente.

> **Note**
>
> Le chiavi di attivazione dell'agente scadono dopo 30 minuti se non vengono utilizzate.

DataSync console

Quando attivi l'agente nella DataSync console, DataSync puoi ottenere la chiave di attivazione utilizzando l'opzione Ottieni automaticamente la chiave di attivazione dal tuo agente.

Per utilizzare questa opzione, il browser deve essere in grado di contattare l'agente sulla porta 80.

Agent local console

A differenza delle altre opzioni per ottenere una chiave di attivazione, questa opzione non richiede che l'agente sia accessibile sulla porta 80.

1. Accedi alla console locale della tua macchina virtuale (VM) agente o dell' EC2istanza Amazon.
2. Nel menu principale AWS DataSync Attivazione - Configurazione, accedi **0** per ottenere una chiave di attivazione.
3. Inserisci il codice in Regione AWS cui stai attivando il tuo agente.
4. Inserisci il tipo di endpoint di servizio utilizzato dal tuo agente.
5. Copia la chiave di attivazione visualizzata.

   Ad esempio: `F0EFT-7FPPR-GG7MC-3I9R3-27D0H`

   Specificate questa chiave quando attivate il vostro agente.

CLI

Con gli strumenti Unix standard, puoi `curl` inviare una richiesta all'indirizzo IP del tuo agente per ottenere la chiave di attivazione.

Per utilizzare questa opzione, il client deve essere in grado di contattare l'agente sulla porta 80. È possibile eseguire il seguente comando per verificare:

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

Dopo aver confermato di poter contattare l'agente, esegui uno dei seguenti comandi a seconda del tipo di endpoint di servizio che stai utilizzando:

- Endpoint di servizio pubblico:

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

- Endpoint del servizio FIPS:

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

- Endpoint del servizio VPC:

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

  Per trovarli*vpc-endpoint-ip-address*, apri la console Amazon VPC, scegli Endpoints e seleziona l'endpoint del servizio VPC DataSync . Nella scheda Subnet, individua l'indirizzo IP per la sottorete dell'endpoint del servizio VPC. Questo è l'indirizzo IP dell'endpoint.

Questo comando restituisce una chiave di attivazione. Per esempio:

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

Specificate questa chiave quando attivate il vostro agente.

Attivazione del tuo agente

Hai diverse opzioni per attivare il tuo DataSync agente. Una volta attivato, AWS gestisce l'agente per te.

DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Agenti, quindi scegli Crea agente.
3. Nella sezione Service endpoint, procedi come segue per specificare l'endpoint di servizio per il tuo agente:

   - Per un endpoint di servizio pubblico, scegli Endpoint di servizio pubblico in. *your current Regione AWS*
   - Per un endpoint del servizio FIPS, scegli gli endpoint del servizio FIPS in. *your current Regione AWS*
   - Per un endpoint del servizio VPC, procedi come segue:
     - Scegli gli endpoint VPC utilizzando. AWS PrivateLink
     - Per l'endpoint VPC, scegli l'endpoint del servizio VPC che desideri venga utilizzato dal tuo agente.
     - Per Subnet, scegli la sottorete in cui si trova l'endpoint del servizio VPC.
     - Per il gruppo di sicurezza, scegli il gruppo di sicurezza che consente il traffico richiesto per l'utilizzo degli endpoint del servizio DataSync VPC.
4. Nella sezione Chiave di attivazione, esegui una delle seguenti operazioni per specificare la chiave di attivazione del tuo agente:

   - Scegli Ottieni automaticamente la chiave di attivazione dal tuo agente DataSync per ottenere la chiave per te.
     - Per l'indirizzo dell'agente, inserisci l'indirizzo IP o il nome di dominio dell'agente.
     - Scegli Ottieni chiave.

       Se l'attivazione fallisce, controlla la configurazione della rete in base al tipo di endpoint di servizio che stai utilizzando.
   - Scegli Inserisci manualmente la chiave di attivazione dell'agente se non desideri una connessione tra il browser e l'agente.
     - Ottieni la chiave dalla console locale dell'agente o utilizzando un `curl` comando.

- Tornando alla DataSync console, inserisci la chiave nel campo Chiave di attivazione.

5. (Consigliato) Per il nome dell'agente, assegna al tuo agente un nome facile da ricordare.
6. (Facoltativo) Per i tag, inserisci i valori nei campi Chiave e Valore per etichettare il tuo agente.

   I tag ti aiutano a gestire, filtrare e cercare AWS le tue risorse.
7. Scegliere Create agent (Crea agente).
8. Nella pagina Agenti, verifica che l'agente stia utilizzando il tipo di endpoint di servizio corretto.

> **Note**
>
> A questo punto, potresti notare che il tuo agente è offline. Ciò accade brevemente dopo l'attivazione di un agente.

AWS CLI

1. Una volta ottenuta la chiave di attivazione, copia uno dei seguenti `create-agent` comandi a seconda del tipo di endpoint di servizio che stai utilizzando:

   - Endpoint di servizio pubblico o FIPS:

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

   - Endpoint del servizio VPC:

```
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. Per`--activation-key`, specifica la chiave di attivazione dell'agente.
3. (Consigliato) Per`--agent-name`, specifica un nome facile da ricordare per il tuo agente.
4. Se utilizzi un endpoint del servizio VPC, specifica le seguenti opzioni:

   - Per`--vpc-endpoint-id`, specifica l'ID dell'endpoint del servizio VPC che stai utilizzando.

- Per `--subnet-arns`, specifica l'ARN della sottorete in cui si trova l'endpoint del servizio VPC.
- Per `--security-group-arns`, specifica l'ARN del gruppo di sicurezza che consente il traffico richiesto per l'utilizzo degli endpoint del servizio DataSync VPC.

5. Esegui il comando `create-agent`.

   Riceverai una risposta con l'ARN dell'agente che hai appena attivato. Per esempio:

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

6. Verifica che il tuo agente sia attivato eseguendo il `list-agents` comando:

   ```
   aws datasync list-agents
   ```

   > **Note**
   >
   > A questo punto, potresti notare che il tuo agente lo `Status` è`OFFLINE`. Ciò accade brevemente dopo l'attivazione di un agente.

DataSync API

Una volta ottenuta la chiave di attivazione, attiva l'agente utilizzando l'CreateAgentoperazione.

> **Note**
>
> Quando hai finito, potresti notare che il tuo agente è offline. Ciò accade brevemente dopo l'attivazione di un agente.

Passaggi successivi

- Verifica la connessione dell'agente al sistema di storage e al DataSync servizio.
- Se riscontri problemi durante il tentativo di attivare l'agente, richiedi assistenza per la risoluzione dei problemi.

- Crea la DataSync sede che desideri utilizzare con il tuo agente. Potrebbe trattarsi di una posizione locale o di altro tipo nel cloud.

Verifica delle connessioni di rete del tuo agente

Una volta attivato l' AWS DataSync agente, assicurati che l'agente disponga di connettività di rete al sistema di storage e al DataSync servizio.

Accesso alla console locale dell'agente

Il modo in cui accedi alla console locale del tuo agente dipende dal tipo di agente che stai utilizzando.

Accesso alla console locale (VMware ESXiLinux KVM o Microsoft Hyper-V)

Per motivi di sicurezza, non è possibile connettersi in remoto alla console locale della macchina virtuale (VM) dell' DataSync agente.

- Se è la prima volta che utilizzi la console locale, accedi con le credenziali predefinite. Il nome utente predefinito è **`admin`** e la password è **`password`**.

  > **Note**
  >
  > Consigliamo di modificare la password predefinita. Per fare ciò, nel menu principale della console inserisci **`5`** (o **`6`** per VMware VMs), quindi esegui il `passwd` comando per modificare la password.

Accesso alla console locale (Amazon EC2)

Per connetterti alla console locale di un EC2 agente Amazon, devi usare SSH.

Prima di iniziare: assicurati che il gruppo di sicurezza dell' EC2istanza consenta l'accesso con SSH (porta TCP 22).

1. Apri un terminale e copia il seguente comando: `ssh`

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

   - Per*`/path/key-pair-name`*, specifica il percorso e il nome del file (`.pem`) della chiave privata richiesta per connetterti all'istanza.

- Per *instance-user-name*, specificare `admin`.
- Per*instance-public-ip-address*, specifica l'indirizzo IP pubblico dell'istanza.

2. Esegui il `ssh` comando per connetterti all'istanza.

Una volta connesso, viene visualizzato il menu principale della console locale dell'agente.

Verifica della connessione dell'agente al sistema di storage

Verifica se l' DataSync agente è in grado di connettersi al sistema di storage. Per ulteriori informazioni, consulta 1. Connessione di rete tra il sistema di storage e l'agente.

1. Accedi alla console locale del tuo agente.
2. Nel menu principale AWS DataSync Attivazione - Configurazione, inserisci**3**.
3. Immettete una delle seguenti opzioni:

   a. Entra **1** per testare una connessione al server NFS.

   b. Invio **2** per testare una connessione al server SMB.

   c. Invio **3** per testare una connessione al server di storage di oggetti.

   d. Entra **4** per testare una connessione HDFS.

   e. Entra **5** per testare una Microsoft Azure Blob Storage connessione.

4. Immettere l'indirizzo IP o il nome di dominio del server di storage.

   Quando inserisci l'indirizzo IP o il nome di dominio, ricorda quanto segue:

   - Non includere un protocollo. Ad esempio, inserisci **`mystorage.com`** invece di**`https://mystorage.com`**.
   - Per HDFS, inserisci l'indirizzo IP o il nome di dominio di NameNode o DataNode nel cluster Hadoop.

5. Se richiesto, inserire la porta TCP per la connessione al server di archiviazione (ad esempio,). **`443`**

Verifica se il test di connettività è stato SUPERATO o FALLITO.

Verifica della connessione del tuo agente al servizio DataSync

Verifica se il tuo DataSync agente è in grado di connettersi al DataSync servizio. Per ulteriori informazioni, consulta 2. Connessione di rete tra l'agente e DataSync il servizio.

1. Accedi alla console locale del tuo agente.
2. Nel menu principale AWS DataSync Attivazione - Configurazione, accedi **2** per iniziare a testare la connettività di rete.

   Se l'agente è attivato, l'opzione Test Network Connectivity può essere avviata senza alcun input aggiuntivo da parte dell'utente, poiché la regione e il tipo di endpoint vengono presi dalle informazioni sull'agente attivato.
3. Inserisci il tipo di endpoint di DataSync servizio utilizzato dal tuo agente:

   a. Per gli endpoint del servizio pubblico, inserisci **1** e il Regione AWS luogo in cui è attivato il tuo agente.
   b. Per gli endpoint del servizio FIPS, inserisci **2** la regione in cui è attivato l'agente.
   c. Per gli endpoint del servizio VPC, immettere. **3**

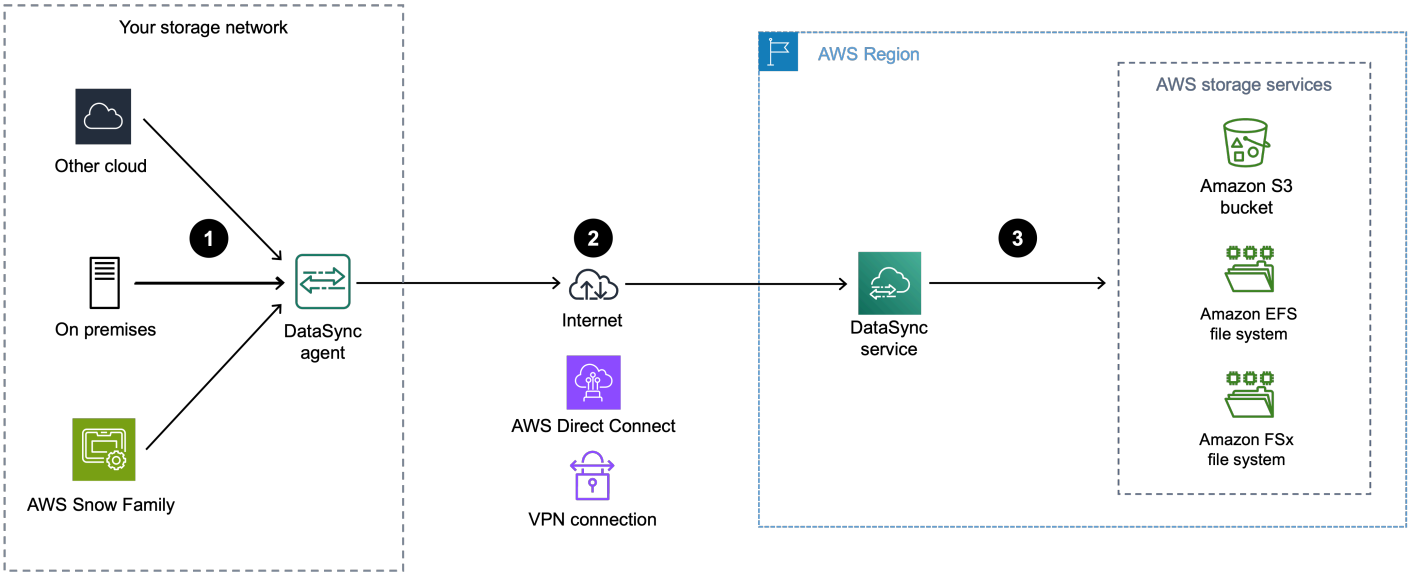
   Viene visualizzato un messaggio PASSATO o FALLITO.
4. Se viene visualizzato un messaggio FAILED, controlla la configurazione di rete. Per ulteriori informazioni, consulta AWS DataSync requisiti di rete.

Passaggi successivi

Crea la DataSync posizione che desideri utilizzare con il tuo agente. Potrebbe trattarsi di una posizione locale o di altro tipo nel cloud.

Connessione della rete per AWS DataSync i trasferimenti

Se è necessario un AWS DataSync agente, è necessario stabilire diverse connessioni di rete per il trasferimento dei dati. Il diagramma seguente mostra le tre connessioni di rete in un DataSync trasferimento da un sistema di storage (che potrebbe essere locale, in un altro cloud o all'edge) a un servizio di AWS storage.



1. Connessione di rete tra il sistema di storage e l'agente

Il tuo DataSync agente si connette al tuo sistema di storage locale, a un altro sistema di archiviazione cloud o edge. Per ulteriori informazioni, consulta Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge.

2. Connessione di rete tra l'agente e DataSync il servizio

Esistono alcuni aspetti per connettere il tuo agente al DataSync servizio. Innanzitutto, è necessario connettere la rete di storage a AWS. In secondo luogo, l'agente necessita di un endpoint di servizio con DataSync cui comunicare.

Indice

- Connessione della rete di storage a AWS
- Selezione di un endpoint del servizio

Connessione della rete di storage a AWS

Durante l'utilizzo DataSync, considera le seguenti opzioni per connettere la rete di storage a AWS:

- AWS Direct Connect- Con Direct Connect, è possibile creare una connessione dedicata tra la rete di storage e AWS. Da un DataSync punto di vista, ciò consente di:
  - Trasferisci i dati su un percorso privato verso il tuo cloud privato virtuale (VPC), che evita il routing sulla rete Internet pubblica.
  - Ottieni una connessione più prevedibile rispetto all'utilizzo di una rete privata virtuale (VPN) a cui connettere la tua rete di storage AWS (in particolare se il tuo agente è un' EC2 istanza Amazon).
  - Utilizza qualsiasi tipo di endpoint di DataSync servizio, inclusi gli endpoint pubblici, FIPS (Federal Information Processing Standard) o VPC.

  Per ulteriori informazioni, consulta DataSync esempi di architettura e routing con AWS Direct Connect.
- VPN: puoi connettere la tua rete di archiviazione AWS utilizzando una VPN (ad esempio). AWS Site-to-Site VPN
- Internet pubblico: è possibile connettere la rete di archiviazione direttamente a DataSync Internet utilizzando un endpoint di servizio pubblico o FIPS.

Selezione di un endpoint del servizio

L'agente utilizza un endpoint di servizio con cui comunicare. DataSync Per ulteriori informazioni, consulta Scelta di un endpoint di servizio per il tuo agente AWS DataSync.

3. Connessione di rete tra il DataSync servizio e il servizio AWS di archiviazione

Per connetterti DataSync a un servizio di AWS storage, devi solo assicurarti che il DataSync servizio possa accedere al tuo bucket o file system S3. Per ulteriori informazioni, consulta Requisiti di rete per i servizi AWS di storage.

Collegamento in rete quando non è necessario un agente DataSync

Per i trasferimenti che non richiedono un DataSync agente, è sufficiente assicurarsi che il DataSync servizio possa accedere ai sistemi di AWS storage tra i quali si effettua il trasferimento. Per ulteriori informazioni, consulta Requisiti di rete per i servizi AWS di storage.

Come e dove scorre DataSync il traffico attraverso la rete

DataSync dispone di un piano dati e di un piano di controllo del traffico. Sapere come ognuno di questi fluisce attraverso la rete è importante se si desidera separare il DataSync traffico.

- Traffico sul piano dati: include i dati di file o oggetti che si spostano tra le posizioni di archiviazione. Nella maggior parte dei casi, il traffico del piano dati viene indirizzato attraverso interfacce di rete che generano e gestiscono DataSync automaticamente quando si crea un'attività. Il luogo in cui vengono create queste interfacce di rete dipende dal tipo di servizio di AWS storage verso o da cui si effettua il trasferimento e dall'endpoint di servizio utilizzato dall'agente. DataSync
- Controlla il traffico aereo: include le attività di gestione delle risorse. DataSync Questo traffico viene indirizzato attraverso l'endpoint di servizio utilizzato dall'agente.

Sicurezza di rete per DataSync

Per informazioni su come vengono protetti i dati di archiviazione (inclusi i metadati) durante un trasferimento, consulta. AWS DataSync crittografia in transito

AWS DataSync requisiti di rete

La configurazione della rete è un passaggio importante nella configurazione. AWS DataSync La configurazione di rete dipende da diversi fattori, ad esempio il tipo di sistemi di storage con cui state lavorando. Si basa anche sul tipo di endpoint di DataSync servizio che intendi utilizzare.

IPv6 supporto

DataSync dispone del supporto dual-stack per la compatibilità con entrambe le IPv4 reti. IPv6 IPv6 il supporto è disponibile in tutti i paesi in Regioni AWS cui viene offerto il servizio. DataSync supporta l'utilizzo di IPv6 indirizzi con le seguenti fonti di dati:

- Network File System (NFS)
- Server Message Block (SMB)
- Archiviazione di oggetti

IPv6-agenti compatibili

Per poterlo utilizzare DataSync in un ambiente IPv6 di rete, è necessario utilizzare agenti IPv6 compatibili. Questi agenti supportano sia la connettività che IPv4 la IPv6 connettività, adattandosi a vari ambienti di rete.

- IPv6Solo per reti: non sono necessarie modifiche alla configurazione.
- IPv4Solo per reti: non è richiesta alcuna modifica alla configurazione.
- Per le reti dual-stack (IPv4 sia che IPv6), consenti all'agente di selezionare il protocollo o configurarlo manualmente in base alle tue preferenze.

Considerazioni per le reti dual-stack

Puoi personalizzare il comportamento del tuo agente tramite la console locale nei seguenti modi:

- Disabilita IPv6 in modo che l'agente non possa IPv6 utilizzare per raggiungere i file system locali o il servizio. DataSync
- Imposta la versione IP dell'agente da utilizzare per i trasferimenti di dati:
  - Impostato in IPv6 modo che l'agente lo utilizzi solo IPv6 per i trasferimenti di dati.
  - Impostare IPv4 in modo che l'agente lo utilizzi solo IPv4 per i trasferimenti di dati.
  - Imposta su Auto (ripristina l'impostazione predefinita) in modo che l'agente scelga automaticamente la versione (IPv4 o IPv6) del protocollo per i trasferimenti di dati.

Per ulteriori informazioni sulla gestione delle impostazioni della versione IP dell'agente, vederethe section called “Esecuzione della manutenzione del vostro agente”.

> **Important**
>
> Gli agenti creati a partire da immagini scaricate prima del 16 luglio 2025 non supportano IPv6.

Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge

I seguenti requisiti di rete possono essere applicati ai sistemi di storage on-premise, autogestiti, ad altri sistemi di storage cloud ed edge. Si tratta in genere di sistemi di storage che gestisci o che potrebbero essere gestiti da un altro provider di servizi cloud.

> **Note**
>
> A seconda della rete, potrebbe essere necessario consentire il traffico su porte diverse da quelle elencate qui per consentire all' DataSync agente di connettersi allo storage.

Da	Per	Protocollo	Porta	Come viene utilizzato da DataSync
DataSync agente	file server NFS	TCP	2049 (per le versioni NFS 4.1 e 4.0) 111 e 2049 (per la versione 3.x di NFS)	Monta il file server NFS. DataSync supporta le versioni NFS 3.x, 4.0 e 4.1.
DataSync agente	file server SMB	TCP	139 o 445	Monta il file server SMB. DataSync supporta le versioni SMB 1.0 e successive. Per motivi di sicurezza, consigliamo di utilizzare la versione 3.0.2 o successiva di SMB. Le versioni precedenti, come SMB 1.0, contengono vulnerabilità di sicurezza note che gli aggressor

Da	Per	Protocollo	Porta	Come viene utilizzato da DataSync
				i possono sfruttare per compromettere i dati.

Da	Per	Protocollo	Porta	Come viene utilizzato da DataSync
DataSync agente	Archiviazione di oggetti	TCP	443 (HTTPS) o 80 (HTTP) **Note** A second dell'arcl iviazion degli oggetti, potrebb essere necessa o consen e il traffico su porte HTTPS e HTTP non standar (ad esempi 8443 o 8080).	Accedi allo storage di oggetti compatibile con Amazon S3 in locale o in altri cloud.

Da	Per	Protocollo	Porta	Come viene utilizzato da DataSync
DataSync agente	cluster Hadoop	TCP	NameNode porta (l'impostazione predefinita è 8020) Nella maggior parte dei cluster, è possibile trovare questo numero di porta nel `core-site.xml` file sotto la `fs.default.name` proprietà `fs.default` o (a seconda della distribuzione Hadoop).	Accede a NameNodes nel tuo cluster Hadoop. Specificate la porta utilizzata per la creazione di una posizione HDFS.

Da	Per	Protocollo	Porta	Come viene utilizzato da DataSync
DataSync agente	cluster Hadoop	TCP	DataNode porta (l'impostazione predefinita è 50010) Nella maggior parte dei cluster, è possibile trovare questo numero di porta nel `hdfs-site.xml` file sotto la `dfs.datanode.address` proprietà.	Accede a DataNodes nel tuo cluster Hadoop. L' DataSyncagente determina automaticamente la porta da utilizzare.
DataSync agente	Server di gestione delle chiavi Hadoop (KMS)	TCP	Porta KMS (l'impostazione predefinita è 9600)	Accede al KMS per il tuo cluster Hadoop.

Da	Per	Protocollo	Porta	Come viene utilizzato da DataSync
DataSync agente	server Kerberos Key Distribution Center (KDC)	TCP	Porta KDC (l'impost azione predefinita è 88)	Si autentica con il realm Kerberos. Questa porta viene utilizzata solo con posizioni HDFS e SMB che utilizzano l'autenti cazione Kerberos.
DataSync agente	interfaccia di gestione del sistema di storage	TCP	Dipende dalla rete in uso	Si connette al sistema di storage.

Requisiti di rete per i servizi AWS di storage

Le porte di rete necessarie per DataSync connettersi a un servizio AWS di storage durante un trasferimento variano.

Da	Per	Protocollo	Porta
DataSync servizio	Amazon EFS	TCP	2049
DataSync servizio	FSx per Windows File Server	Vedi controllo dell'accesso al file system FSx per Windows File Server.	
DataSync servizio	FSx per Lustre	Vedi il controllo degli accessi al file system FSx per Lustre.	
DataSync servizio	FSx per OpenZFS	Vedi il controllo degli accessi al file system FSx per OpenZFS.	
DataSync servizio	FSx per ONTAP	TCP	111, 635 e 2049 (NFS) 445 (SMB)

Da	Per	Protocollo	Porta
DataSync servizio	Amazon S3	N/A (DataSync si connette ai bucket S3 per tuo conto)	

Requisiti di rete per gli endpoint di servizio pubblici o FIPS

DataSync L'agente richiede il seguente accesso alla rete quando utilizza endpoint di servizio pubblici o FIPS. Se utilizzi un firewall o un router per filtrare o limitare il traffico di rete, configura il firewall o il router per consentire questi endpoint.

Da	Per	Protocollo	Porta	Come viene usato	Endpoint accessibili
Browser	DataSync agente	TCP	80 (HTTP)	Consente al browser di ottenere la chiave di attivazione dell' DataSync agente. Una volta attivata, DataSync chiude la porta 80 dell'agente. Il tuo agente non richiede che la porta 80 sia accessibile al pubblico. Il livello di accesso richiesto alla porta 80 dipende dalla	N/D

Da	Per	Protocollo	Porta	Come viene usato	Endpoint accessibili
				configurazione di rete. **Note** Puoi ottenere la chiave di attivazione senza una connessione tra il browser e l'agente. Per ulteriori informazioni, consulta Ottenere una chiave di attivazione.	

Da	Per	Protocollo	Porta	Come viene usato	Endpoint accessibili
DataSync agente	Amazon CloudFront	TCP	443 (HTTPS)	Consente di avviare l' DataSync agente prima dell'attivazione.	Regioni AWS: • `d3dvvaliwoko8h.cloudfront.net` AWS GovCloud (US) Regioni: • `s3.us-gov-west-1.amazonaws.com/fmrsendpoints-endpointsbucket-go4p5gpna6sk`
DataSync agente	AWS	TCP	443 (HTTPS)	Attiva il tuo DataSync agente e lo associa al tuo. Account AWSÈ possibile bloccare l'endpoint pubblico dopo l'attivazione.	*`activation-region`* È Regione AWS qui che attivi il tuo DataSync agente. Attivazione pubblica degli endpoint: • `activation.datasync.` *`activation-region`*`.amazonaws.com` Attivazione degli endpoint FIPS: • `activation.datasync-fips.` *`activation-region`*`.amazonaws.com`

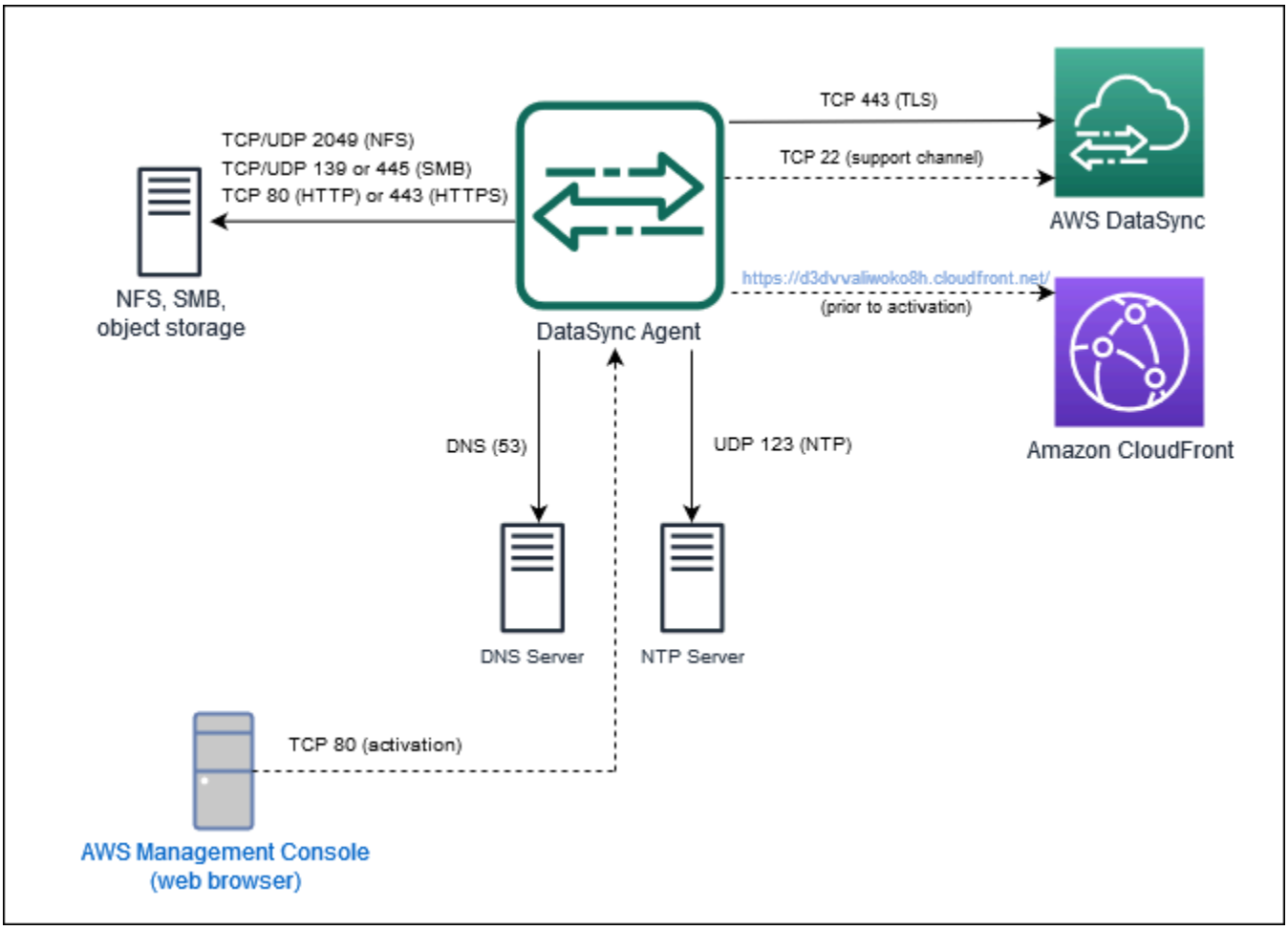
Da	Per	Protocollo	Porta	Come viene usato	Endpoint accessibili
DataSync agente	AWS	TCP	443 (HTTPS)	Consente la comunicazione tra l' DataSync agente e l'endpoint DataSync del servizio. Per informazioni, consultare Scelta di un endpoint di servizio per il tuo agente AWS DataSync.	*activation-region* È il Regione AWS luogo in cui attivi il tuo DataSync agente. A seconda dell'uso che utilizzi DataSync , potrebbe non essere necessari o consentire l'accesso a tutti gli endpoint elencati qui. DataSync estremità del piano di controllo: • Endpoint pubblico: `cp.datasync.` *activation-region* `.amazonaws.com` • Endpoint FIPS: `cp.datasync-fips.` *activation-region* `.amazonaws.com` DataSync endpoint del piano dati (solo per le attività di trasferimento): • *your-task-id* `.datasync-dp.` *activation-region* `.amazonaws.com`

Da	Per	Protocollo	Porta	Come viene usato	Endpoint accessibili
Il tuo cliente	AWS	TCP	443 (HTTPS)	Ti consente di effettuare richieste DataSync API.	*activation-region* È il Regione AWS luogo in cui attivi il tuo DataSync agente. Endpoint pubblico: • `datasync.` *activation-region* `.amazonaws.com` Endpoint FIPS: • `datasync-fips.` *activation-region* `.amazonaws.com`

Da	Per	Protocollo	Porta	Come viene usato	Endpoint accessibili
DataSync agente	AWS	TCP	443 (HTTPS)	Consente all' DataSync agente di ricevere aggiornamenti da AWS. Per ulteriori informazioni, consulta Gestire il tuo AWS DataSync agente.	*activation-region* È il Regione AWS luogo in cui attivi il tuo DataSync agente. • amazonlinux.default.amazonaws.com • cdn.amazonlinux.com • amazonlinux-2-repos- *activation-region* .s3.dualstack. *activation-region*.amazonaws.com • amazonlinux-2-repos- *activation-region*.s3.*activation-region*.amazonaws.com • *.s3.*activation-region*.amazonaws.com • *.s3.dualstack. *activation-region*.amazonaws.com
DataSync agente	Server DNS (Domain Name Service)	TCP/UDP	53 (DNS)	Consente la comunicazione tra l' DataSync agente e il server DNS.	N/D

Da	Per	Protocollo	Porta	Come viene usato	Endpoint accessibili
DataSync agente	AWS	TCP	22 (Canale di supporto)	Consente di accedere Supporto AWS al tuo DataSync agente per aiutarti a risolvere i problemi. Non è necessario che questa porta sia aperta per il normale funzionamento.	Supporto AWS canale: • `54.201.223.107`
DataSync agente	Server NTP (Network Time Protocol)	UDP	123 (NTP)	Consente ai sistemi locali di sincronizzare l'ora della macchina virtuale con l'ora dell'host.	NTP: • `0.amazon.pool.ntp.org` • `1.amazon.pool.ntp.org` • `2.amazon.pool.ntp.org` • `3.amazon.pool.ntp.org` **Note** Per modificare la configurazione NTP predefinita dell'agente VM per utilizzare un server NTP diverso utilizzando la console locale, vedere. Sincronizzazione dell'ora sul tuo agente VMware

Il diagramma seguente mostra le porte richieste DataSync quando si utilizzano endpoint di servizio pubblici o FIPS.



Requisiti di rete per gli endpoint del servizio VPC

Un endpoint di cloud privato virtuale (VPC) fornisce una connessione privata tra il tuo agente e AWS che non attraversa Internet né utilizza indirizzi IP pubblici. Questo aiuta anche a impedire che i pacchetti entrino o escano dalla rete. Per ulteriori informazioni, consulta Scelta di un endpoint di servizio VPC.

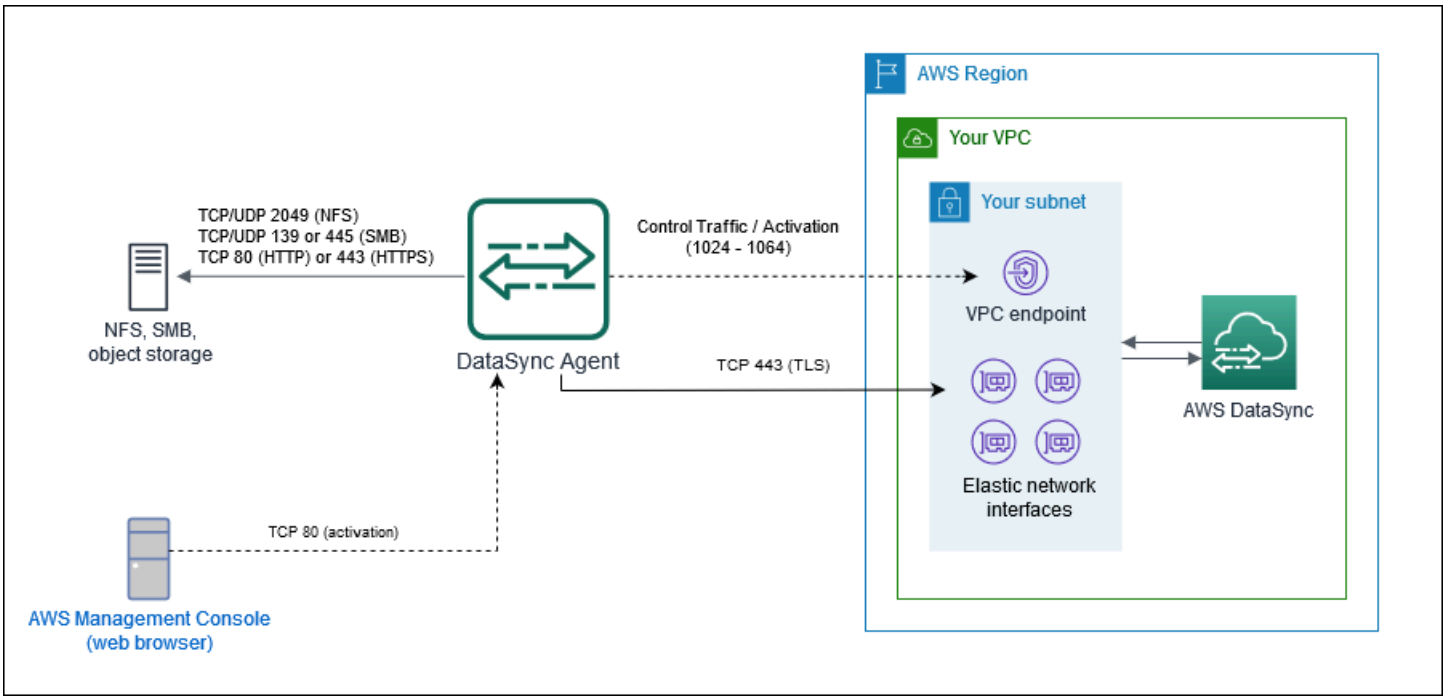
DataSync richiede le seguenti porte affinché l'agente possa utilizzare un endpoint del servizio VPC.

Da	Per	Protocollo	Porta	Come viene usato
Browser	Il tuo DataSync agente	TCP	80 (HTTP)	Consente al browser di ottenere la chiave di attivazione dell'agen

Da	Per	Protocollo	Porta	Come viene usato
				te. Una volta attivata, DataSync chiude la porta 80 dell'agente. Il tuo agente non richiede che la porta 80 sia accessibile al pubblico. Il livello di accesso richiesto alla porta 80 dipende dalla configurazione di rete. **Note** Puoi ottenere la chiave di attivazione senza una connessione tra il browser e l'agente. Per ulteriori informazioni, consulta Ottenere una chiave di attivazione.

Da	Per	Protocollo	Porta	Come viene usato
DataSync agente	Il tuo DataSync endpoint di servizio VPC Per trovare l'indirizzo IP dell'endpoint, apri la console Amazon VPC, scegli Endpoints e seleziona l'endpoint del servizio DataSync VPC. Nella scheda Subnet, individua l'indirizzo IP per la sottorete dell'endpoint del servizio VPC. Questo è l'indirizzo IP dell'endpoint.	TCP	1024-1064	Per il controllo del traffico aereo.
DataSync agente	le interfacce di rete della tua DataSync attività Per trovare gli indirizzi IP di queste interfacce, vedi. Visualizzazione delle interfacce di rete	TCP	443 (HTTPS)	Per il traffico dati sul piano dati.
DataSync agente	Il tuo DataSync endpoint di servizio VPC	TCP	22 (Canale di supporto)	Per consentire l'accesso Supporto AWS al proprio DataSync agente per la risoluzione dei problemi. Non è necessario che questa porta sia aperta per il normale funzionamento.

Il diagramma seguente mostra le porte richieste DataSync quando si utilizzano gli endpoint del servizio VPC.



Interfacce di rete per i trasferimenti AWS DataSync

Per ogni attività creata, genera e gestisce AWS DataSync automaticamente le interfacce di rete per il traffico di trasferimento dati. Quante interfacce di rete vengono DataSync create e dove vengono create dipendono dai seguenti dettagli sull'attività di trasferimento:

- Se l'attività richiede un DataSync agente.
- Le tue posizioni di origine e di destinazione (da e verso le quali copi i dati).
- Il tipo di endpoint di servizio utilizzato dal tuo agente.

Ogni interfaccia di rete utilizza un singolo indirizzo IP nella sottorete (maggiore è il numero di interfacce di rete, maggiore è il numero di indirizzi IP necessari). Utilizza le seguenti tabelle per assicurarti che la sottorete disponga di indirizzi IP sufficienti per l'attività.

Interfacce di rete per i trasferimenti con agenti

In generale, è necessario un DataSync agente per copiare dati tra un servizio di AWS storage e un sistema di storage che non lo è. AWS

Ubicazione	Interfacce di rete create per impostazione predefinita	Dove vengono create le interfacce di rete quando si utilizza un endpoint pubblico o FIPS	Dove vengono create le interfacce di rete quando si utilizza un endpoint privato (VPC)
Amazon S3	4	N/A [1]	La sottorete specificata durante l'attivazione dell'agente. DataSync
Amazon EFS	4	La sottorete specificata durante la creazione della posizione Amazon EFS.	
File server Amazon FSx per Windows	4	La stessa sottorete del file server preferito del file system.	
Amazon FSx per Lustre	4	La stessa sottorete del file system.	
Amazon FSx per OpenZFS	4	La stessa sottorete del file system.	
Amazon FSx per NetApp ONTAP	4	La stessa sottorete del file system.	

[1] Le interfacce di rete non sono necessarie perché il DataSync servizio comunica direttamente con il bucket S3.

Interfacce di rete per trasferimenti senza agenti

Non è necessario un DataSync agente per copiare i dati tra di loro. Servizi AWS

Il numero totale di interfacce di rete dipende dalle DataSync posizioni in cui viene effettuato il trasferimento. Ad esempio, il trasferimento tra i file system Amazon EFS e FSx for Lustre richiede quattro interfacce di rete. Nel frattempo, il trasferimento tra FSx Windows File Server e un bucket S3 richiede due interfacce di rete.

Ubicazione	Interfacce di rete create per impostazione predefinita	Dove vengono create le interfacce di rete
Amazon S3	N/A [1]	N/A [1]
Amazon EFS	2	La sottorete specificata durante la creazione della posizione Amazon EFS.
FSx per Windows File Server	2	La stessa sottorete del file server preferito per il file system.
FSx per Lustre	2	La stessa sottorete del file system.
FSx per OpenZFS	2	La stessa sottorete del file system.
FSx per ONTAP	2	La stessa sottorete del file system.

[1] Le interfacce di rete non sono necessarie perché il DataSync servizio comunica direttamente con il bucket S3.

Visualizzazione delle interfacce di rete

Per visualizzare le interfacce di rete assegnate all'operazione di DataSync trasferimento, effettuate una delle seguenti operazioni:

- Usa l'operazione. DescribeTask L'operazione restituisce `SourceNetworkInterfaceArns` e `DestinationNetworkInterfaceArns` con risposte simili a queste:

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

  In questo esempio, l'ID dell'interfaccia di rete è`eni-f012345678abcdef0`.
- Nella EC2 console Amazon, cerca l'ID dell'attività (ad esempio`task-f012345678abcdef0`) per trovare le relative interfacce di rete.

DataSync esempi di architettura e routing con AWS Direct Connect

Prendi in considerazione le seguenti architetture di rete quando utilizzi AWS Direct Connecti tuoi trasferimenti. AWS DataSync

> **Tip**
>
> Se la tua rete utilizza un gateway di transito, ti consigliamo di separare il percorso logico del DataSync trasferimento per ottimizzare i costi (in particolare se stai migrando una grande quantità di dati).
> Ad esempio, se utilizzi AWS Transit Gatewayil traffico normale tra le reti locali e i cloud privati virtuali (VPCs), puoi configurare la rete in modo che il DataSync traffico aggiri il gateway di transito e i relativi costi di elaborazione dei dati.

Utilizzo di Direct Connect con un DataSync endpoint di servizio VPC

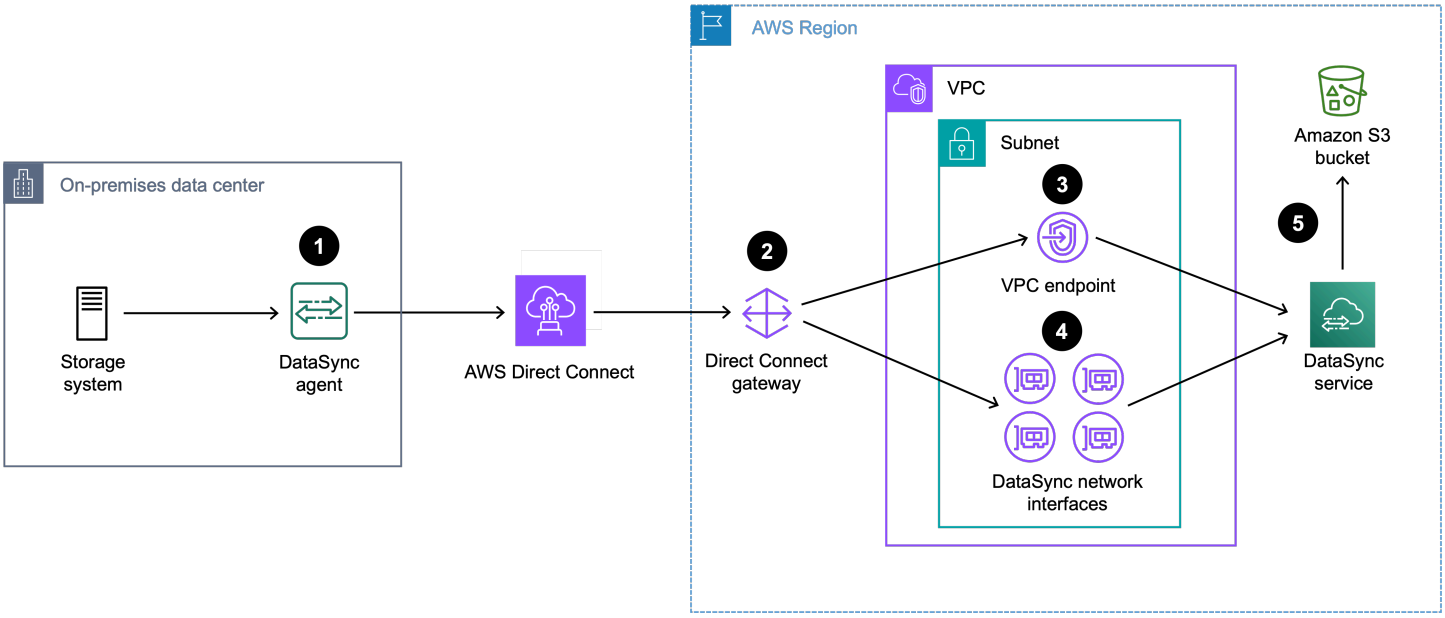
Se il tuo DataSync agente utilizza un endpoint di servizio VPC, hai bisogno di un gateway Direct Connect per connetterti al tuo VPC.

Indice

- Architettura Direct Connect con endpoint VPC e destinazione S3
- Architettura Direct Connect con endpoint VPC e destinazione del file system nella stessa sottorete
- Architettura Direct Connect con endpoint VPC e destinazione del file system in diverse sottoreti

Architettura Direct Connect con endpoint VPC e destinazione S3

La seguente architettura Direct Connect mostra un DataSync trasferimento da un sistema di storage locale a un bucket S3.

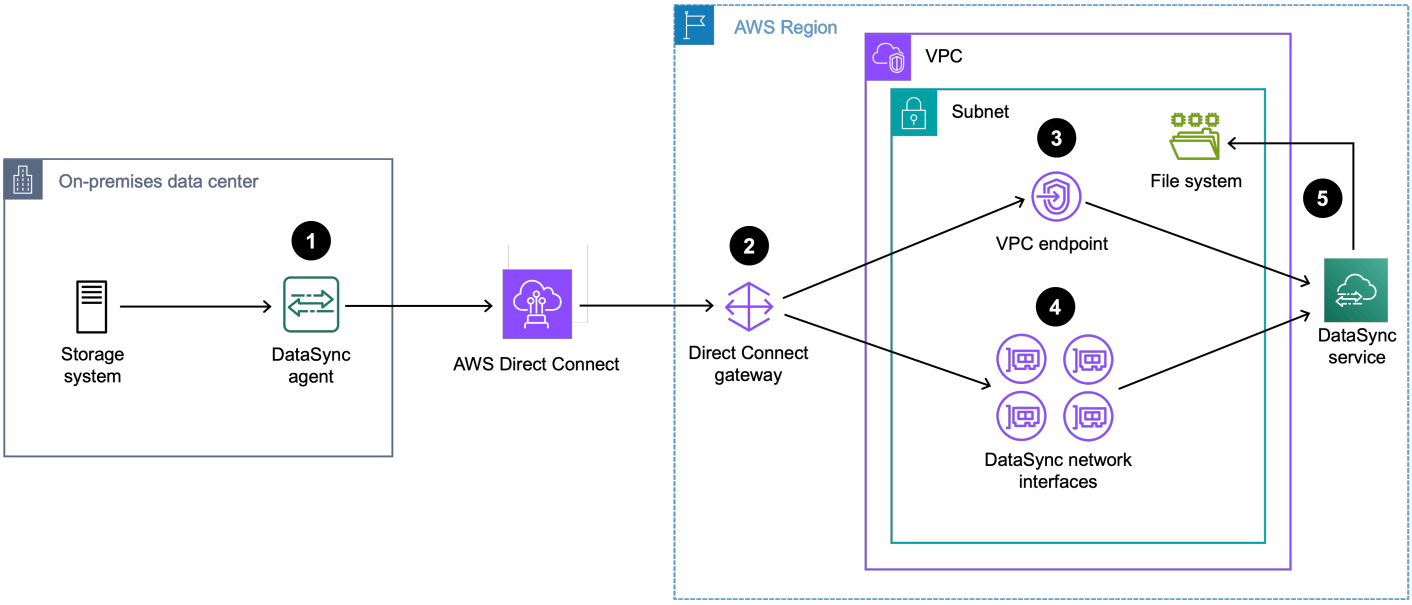


1. L' DataSync agente indirizza il DataSync traffico dal sistema di storage locale (posizione di origine) alla connessione Direct Connect.
2. DataSync il traffico viene indirizzato a un gateway Direct Connect utilizzato per il trasferimento. Per configurarlo, devi:
   a. Associa il gateway Direct Connect a un gateway privato virtuale per il VPC. Questo è il VPC in cui si trova l'endpoint DataSync VPC e dove l'attività crea le DataSync interfacce di rete.
   b. Crea un'interfaccia virtuale privata che colleghi questo VPC al gateway Direct Connect.
3. DataSync percorsi del traffico (piano di controllo) attraverso l' DataSync endpoint VPC.
4. DataSync il traffico (piano dati) viene instradato attraverso le interfacce di DataSync rete nella sottorete specificata durante la creazione dell'agente. DataSync
5. DataSync percorsi di traffico attraverso il DataSync servizio verso il bucket S3 (posizione di destinazione).

Architettura Direct Connect con endpoint VPC e destinazione del file system nella stessa sottorete

Durante il trasferimento da o verso un file system Amazon EFS o Amazon, il FSx file system e l'endpoint DataSync VPC possono trovarsi nella stessa sottorete.

La seguente architettura Direct Connect mostra un DataSync trasferimento da un sistema di storage locale a un FSx file system Amazon EFS o Amazon.

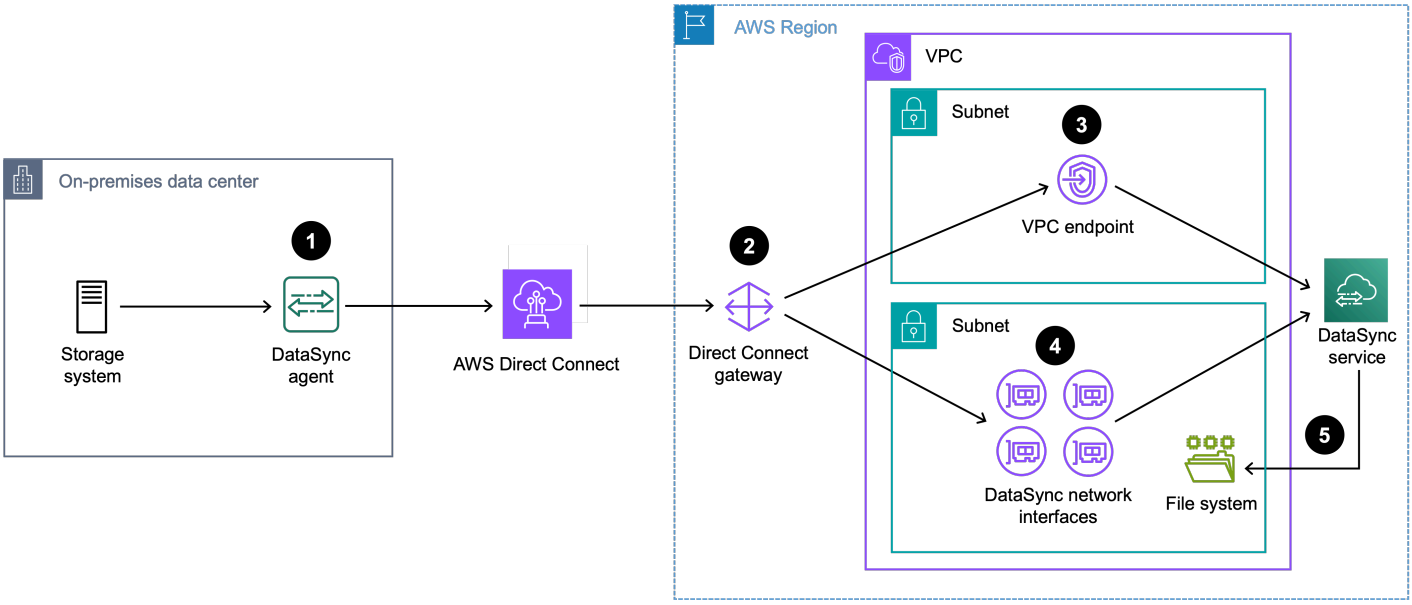


1. L' DataSync agente indirizza il DataSync traffico dal sistema di storage locale (posizione di origine) alla connessione Direct Connect.
2. DataSync il traffico viene indirizzato a un gateway Direct Connect utilizzato per il trasferimento. Per configurarlo, devi:
   a. Associa il gateway Direct Connect a un gateway privato virtuale per il VPC. Questo è il VPC in cui si trova l'endpoint DataSync VPC e dove l' DataSync attività crea interfacce di rete per il file system (posizione di destinazione).
   b. Crea un'interfaccia virtuale privata che colleghi questo VPC al gateway Direct Connect.
3. DataSync percorsi del traffico (piano di controllo) attraverso l' DataSync endpoint VPC.
4. DataSync il traffico (piano dati) viene instradato attraverso le interfacce DataSync di rete nella sottorete del file system. Questa è la stessa sottorete in cui si trova l'endpoint DataSync VPC.
5. DataSync instradamenti del traffico attraverso il DataSync servizio verso il file system (posizione di destinazione).

Architettura Direct Connect con endpoint VPC e destinazione del file system in diverse sottoreti

Durante il trasferimento da o verso un file system Amazon EFS o Amazon, il FSx file system e l'endpoint DataSync VPC possono trovarsi in sottoreti diverse.

La seguente architettura Direct Connect mostra un DataSync trasferimento da un sistema di storage locale a un FSx file system Amazon EFS o Amazon.



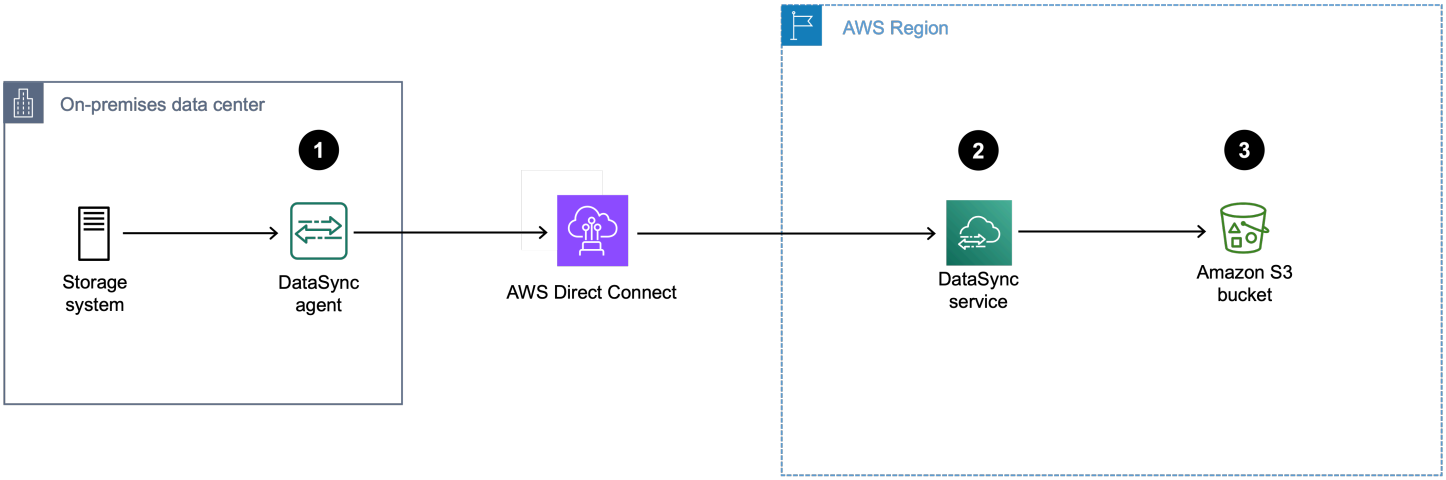
1. L' DataSync agente indirizza il DataSync traffico dal sistema di storage locale (posizione di origine) alla connessione Direct Connect.
2. DataSync il traffico viene indirizzato a un gateway Direct Connect utilizzato per il trasferimento. Per configurarlo, devi:
   a. Associa il gateway Direct Connect a un gateway privato virtuale per il VPC. Questo è il VPC in cui si trova l'endpoint DataSync VPC e dove l' DataSync attività crea interfacce di rete per il file system (posizione di destinazione).
   b. Crea un'interfaccia virtuale privata che li colleghi VPCs al gateway Direct Connect.
3. DataSync percorsi del traffico (piano di controllo) attraverso l' DataSync endpoint VPC.
4. DataSync il traffico (piano dati) viene instradato attraverso le interfacce DataSync di rete nella sottorete del file system. Si tratta di una sottorete diversa da quella in cui si trova l'endpoint DataSync VPC.
5. DataSync i percorsi del traffico attraverso il DataSync servizio verso il file system (posizione di destinazione).

Utilizzo di Direct Connect con un DataSync endpoint di servizio pubblico o FIPS

Se il tuo DataSync agente utilizza un endpoint del servizio FIPS (Federal Information Processing Standard) pubblico o federale, puoi indirizzare il traffico di trasferimento dati tramite una connessione Direct Connect utilizzando un'interfaccia virtuale pubblica.

Sebbene Direct Connect pubblicizzi per impostazione predefinita tutti i Regione AWS prefissi locali e remoti, puoi utilizzare i tag della community BGP per controllare l'ambito (regionale o globale) e le preferenze di indirizzamento del traffico sull'interfaccia virtuale pubblica. Devi pubblicizzare almeno un prefisso pubblico per creare il tuo agente. DataSync

La seguente architettura Direct Connect mostra un DataSync trasferimento da un sistema di storage locale tramite un endpoint pubblico o FIPS a un bucket S3.



1. L' DataSync agente indirizza il DataSync traffico dal sistema di storage locale (posizione di origine) alla connessione Direct Connect.
2. DataSync le rotte di traffico verso il DataSync servizio attraverso un'interfaccia virtuale pubblica.
3. DataSync traffico verso il bucket S3 (posizione di destinazione).

Passaggi successivi

Se hai bisogno di un DataSync agente e non ne hai ancora creato uno, distribuisci l'agente, scegli un endpoint di servizio per l'agente e quindi attiva l'agente.

Una volta creato l'agente, puoi configurare la tua rete per. DataSync

Configurazione del tuo AWS DataSync agente per più NICs

Se si configura l' AWS DataSync agente per utilizzare più adattatori di rete (NICs), è possibile accedere all'agente tramite più di un indirizzo IP. Tale condizione torna utile nei seguenti casi:

- Massimizzazione della velocità effettiva: potresti voler massimizzare la velocità di trasmissione di un agente quando gli adattatori di rete rappresentano un collo di bottiglia.

- Isolamento della rete: il Network File System (NFS), il Server Message Block (SMB), l'Hadoop Distributed File System (HDFS) o il server di archiviazione degli oggetti potrebbero risiedere su una LAN virtuale (VLAN) priva di connettività Internet per motivi di sicurezza.

In un tipico caso di utilizzo con più adattatori, un adattatore è configurato come percorso con cui l'agente comunica (come agente predefinito). AWS Ad eccezione di questo adattatore, NFS, SMB, HDFS o le posizioni di archiviazione di oggetti autogestite devono trovarsi nella stessa sottorete dell'adattatore che si connette a tali adattatori.

In caso contrario, la comunicazione con le posizioni di archiviazione degli oggetti previste per NFS, SMB, HDFS o oggetti potrebbe non essere possibile. In alcuni casi, è possibile configurare una posizione di archiviazione NFS, SMB, HDFS o oggetti sullo stesso adattatore con cui si comunica. AWS In questi casi, il traffico NFS, SMB, HDFS o object storage per quel server e AWS il traffico fluiscono attraverso lo stesso adattatore.

In alcuni casi, è possibile configurare un adattatore per la connessione alla AWS DataSync console e quindi aggiungere un secondo adattatore. In tal caso, configura DataSync automaticamente la tabella delle rotte per utilizzare il secondo adattatore come route preferita.

Trasferimento dei dati con AWS DataSync

Con AWS DataSync, puoi trasferire dati da o verso uno storage locale AWS, in altri cloud e sull'edge.

La configurazione di un DataSync trasferimento prevede in genere i seguenti passaggi:

1. Determina se DataSync supporta il trasferimento.
2. Se hai bisogno di un DataSync agente per il trasferimento, implementa e attiva un agente il più vicino possibile a uno dei tuoi sistemi di storage.

   Ad esempio, se esegui il trasferimento da un file server Network File System (NFS) locale, distribuisci l'agente il più vicino possibile a quel file server.
3. Fornisci DataSync l'accesso al tuo sistema di storage.

   DataSync necessita dell'autorizzazione per leggere o scrivere sul dispositivo di archiviazione (a seconda che lo storage sia una posizione di origine o di destinazione). Ad esempio, scopri come fornire DataSync l'accesso ai file server NFS.
4. Connect la rete per il traffico tra il sistema di storage e DataSync.
5. Crea una posizione per il tuo sistema di storage utilizzando la DataSync console o l' DataSync API. AWS CLI

   Ad esempio, scopri come creare una posizione NFS o una posizione Amazon S3.
6. Ripeti i passaggi 3-5 per creare l'altra sede del trasferimento.
7. Crea e avvia un'attività di DataSync trasferimento che includa le posizioni di origine e di destinazione.

Argomenti

- Con chi posso trasferire i miei dati AWS DataSync?
- Trasferimento da o verso lo storage locale con AWS DataSync
- Trasferimento da o verso AWS lo storage con AWS DataSync
- Trasferimento da o verso un altro spazio di archiviazione cloud con AWS DataSync
- Trasferimento da o verso uno storage compatibile con S3 su Snowball Edge
- Creazione di un'attività per il trasferimento dei dati
- Avvio di un'attività per trasferire i dati

Con chi posso trasferire i miei dati AWS DataSync?

La destinazione in cui è possibile trasferire i dati AWS DataSync dipende dai seguenti fattori:

- Luoghi di origine e destinazione del trasferimento
- Se le tue sedi sono diverse Account AWS
- Se le tue sedi sono diverse Regioni AWS

Trasferimenti supportati nello stesso Account AWS

DataSync supporta i trasferimenti tra le seguenti risorse di archiviazione associate alle stesse Account AWS.

Fonte (da)	Destinazione (verso)
• NFS • SMB • HDFS • Archiviazione di oggetti	• Amazon S3 (it) Regioni AWS • Amazon EFS • File server Amazon FSx per Windows • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP
• Amazon S3 (it) Regioni AWS • Amazon EFS • FSx per Windows File Server • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP	• NFS • SMB • HDFS • Archiviazione di oggetti
• Google Cloud Storage • Microsoft Azure Blob Storage • Microsoft Azure Files • Wasabi Cloud Storage • DigitalOcean Spaces	• Amazon S3 (it) Regioni AWS • Amazon EFS • File server Amazon FSx per Windows • FSx per Lustre • FSx per OpenZFS

Fonte (da)	Destinazione (verso)
• 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	• FSx per ONTAP
• Amazon S3 (it) Regioni AWS • Amazon EFS • File server Amazon FSx per Windows • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP	• 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
• Storage compatibile con Amazon S3 su AWS Snowball Edge	• Amazon S3 (it) Regioni AWS • Amazon EFS • File server Amazon FSx per Windows • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP

Fonte (da)	Destinazione (verso)
• Amazon S3 (it) Regioni AWS • Amazon EFS • FSx per Windows File Server • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP	• Storage compatibile con Amazon S3 su Snowball Edge
• Amazon S3 (it) Regioni AWS • Amazon EFS • FSx per Windows File Server • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP	• Amazon S3 (it) Regioni AWS • Amazon EFS • FSx per Windows File Server • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP
• Amazon S3 (nelle AWS regioni)	• Amazon S3 attivo AWS Outposts
• Amazon S3 attivo AWS Outposts	• Amazon S3 (it) Regioni AWS

Trasferimenti supportati tra Account AWS

DataSync supporta alcuni trasferimenti tra risorse di archiviazione associate a diverse Account AWS.

Fonte (da)	Destinazione (verso)
• Amazon EFS [1] • FSx per Windows File Server [2]	• Amazon EFS • FSx per Windows File Server • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP
• Amazon S3 (it) Regioni AWS	• Amazon S3 (it) Regioni AWS • Amazon EFS

Fonte (da)	Destinazione (verso)
	• FSx per Windows File Server • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP
• Amazon S3 (it) Regioni AWS • Amazon EFS • FSx per Windows File Server • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP	• Amazon S3 (it) Regioni AWS
• NFS • SMB • HDFS • Archiviazione di oggetti	• Amazon S3 (it) Regioni AWS

[1] Configurato come posizione NFS.

[2] Configurato come sede SMB.

Trasferimenti supportati nello stesso Regione AWS

Non ci sono restrizioni per il trasferimento di dati all'interno dello stesso Regione AWS (incluse le regioni che richiedono l'iscrizione). Per ulteriori informazioni, consulta Regioni AWS supportata da. DataSync

Trasferimenti supportati tra Regioni AWS

Tieni presente quanto segue quando trasferisci dati tra le piattaforme Regioni AWS supportate da DataSync:

- Quando effettui il trasferimento tra servizi di AWS archiviazione diversi Regioni AWS, una delle due sedi deve trovarsi nella regione in cui stai utilizzando. DataSync
- Non è possibile effettuare trasferimenti tra regioni con una posizione di archiviazione NFS, SMB, HDFS o oggetti. In queste situazioni, entrambe le sedi di trasferimento devono trovarsi nella stessa regione in cui si attiva l'agente. DataSync
- Con AWS GovCloud (US) le Regioni, puoi:
  - Trasferimenti tra le regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali).
  - Trasferimento tra una AWS GovCloud (US) regione e un'area commerciale Regione AWS, ad esempio Stati Uniti orientali (Virginia settentrionale). Questo tipo di trasferimento richiede un agente per il trasferimento tra Amazon EFS o Amazon FSx file system.

> **Important**
>
> Paghi per i dati trasferiti tra Regioni AWS. Questo trasferimento viene fatturato come trasferimento di dati dalla regione di origine a quella di destinazione. Per ulteriori informazioni, consulta Prezzi di AWS DataSync.

Determinare se il trasferimento richiede un agente DataSync

A seconda dello scenario di trasferimento, potrebbe essere necessario un DataSync agente. Per ulteriori informazioni, consulta Ho bisogno di un AWS DataSync agente?

Trasferimento da o verso lo storage locale con AWS DataSync

Con AWS DataSync, puoi trasferire file e oggetti tra diversi sistemi di storage locali o autogestiti e i seguenti servizi di storage: AWS

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Argomenti

- Configurazione dei AWS DataSync trasferimenti con un file server NFS
- Configurazione dei AWS DataSync trasferimenti con un file server SMB
- Configurazione dei AWS DataSync trasferimenti con un cluster HDFS
- Configurazione dei DataSync trasferimenti con un sistema di archiviazione di oggetti

Configurazione dei AWS DataSync trasferimenti con un file server NFS

Con AWS DataSync, è possibile trasferire dati tra il file server Network File System (NFS) e uno dei seguenti servizi di AWS storage:

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Per configurare questo tipo di trasferimento, devi creare una posizione per il tuo file server NFS. È possibile utilizzare questa posizione come fonte o destinazione di trasferimento.

Fornire DataSync l'accesso ai file server NFS

Per accedere DataSync al file server NFS, è necessario un DataSync agente. L'agente monta un'esportazione sul file server utilizzando il protocollo NFS.

Argomenti

- Configurazione dell'esportazione NFS
- Versioni NFS supportate

Configurazione dell'esportazione NFS

L'esportazione DataSync necessaria per il trasferimento dipende dal fatto che il file server NFS sia una posizione di origine o di destinazione e da come sono configurate le autorizzazioni del file server.

Se il file server è una posizione di origine, deve DataSync solo leggere e navigare tra i file e le cartelle. Se si tratta di una posizione di destinazione, è DataSync necessario l'accesso root per scrivere nella posizione e impostare proprietà, autorizzazioni e altri metadati sui file e sulle cartelle che stai copiando. Puoi utilizzare l'`no_root_squash`opzione per consentire l'accesso root per l'esportazione.

Gli esempi seguenti descrivono come configurare un'esportazione NFS che fornisce l'accesso a DataSync.

Quando il file server NFS è una posizione di origine (accesso root)

Configurate l'esportazione utilizzando il seguente comando, che fornisce permessi di DataSync sola lettura (`ro`) e accesso root (): `no_root_squash`

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

Quando il file server NFS è una posizione di destinazione

Configurate l'esportazione utilizzando il seguente comando, che fornisce i permessi di DataSync scrittura (`rw`) e l'accesso root (`no_root_squash`):

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

Quando il file server NFS è una posizione di origine (nessun accesso root)

Configura l'esportazione utilizzando il comando seguente, che specifica l'ID utente (UID) e l'ID di gruppo (GID) POSIX che, a quanto pare, fornirebbero autorizzazioni di DataSync sola lettura per l'esportazione:

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

Versioni NFS supportate

Per impostazione predefinita, DataSync utilizza la versione NFS 4.1. DataSync supporta anche NFS 4.0 e 3.x.

Configurazione della rete per i trasferimenti NFS

Per il DataSync trasferimento, è necessario configurare il traffico per alcune connessioni di rete:

1. Consenti il traffico sulle seguenti porte dal tuo DataSync agente al tuo file server NFS:

   - Per le versioni 4.1 e 4.0 di NFS: porta TCP 2049
   - Per la versione 3.x di NFS: porte TCP 111 e 2049

   Gli altri client NFS della rete dovrebbero essere in grado di montare l'esportazione NFS che state utilizzando per trasferire i dati. L'esportazione deve essere accessibile anche senza l'autenticazione Kerberos.
2. Configura il traffico per la connessione dell'endpoint del servizio (ad esempio un endpoint VPC, pubblico o FIPS).
3. Consenti il traffico dal DataSync servizio al servizio di AWS storage verso o da cui stai trasferendo.

Creazione della posizione di trasferimento NFS

Prima di cominciare, tieni presente che:

- È necessario un file server NFS da cui trasferire i dati.
- È necessario un DataSync agente in grado di accedere al file server.
- DataSync non supporta la copia degli elenchi di controllo degli accessi di NFS versione 4 ()ACLs.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo. https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per Tipo di posizione, scegli Network File System (NFS).
4. Per gli agenti, scegli l' DataSync agente che può connettersi al tuo file server NFS.

   Puoi scegliere più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .
5. Per il server NFS, inserisci il nome DNS (Domain Name System) o l'indirizzo IP del file server NFS a cui si connette l' DataSyncagente.
6. Per Mount path, inserisci il percorso di esportazione NFS che desideri montare. DataSync

Questo percorso (o una sottodirectory del percorso) è il luogo in cui vengono DataSync trasferiti i dati da o verso. Per ulteriori informazioni, consulta Configurazione dell'esportazione NFS.

7. (Facoltativo) Espandi le impostazioni aggiuntive e scegli una versione NFS specifica DataSync da utilizzare per accedere al file server.

   Per ulteriori informazioni, consulta Versioni NFS supportate.

8. (Facoltativo) Scegliete Aggiungi tag per etichettare la vostra posizione NFS.

   I tag sono coppie chiave-valore che ti aiutano a gestire, filtrare e cercare le tue sedi. È consigliabile creare almeno un tag di nome per la posizione.

9. Scegli Crea località.

Usando il AWS CLI

- Utilizzate il seguente comando per creare una posizione NFS.

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

Per ulteriori informazioni sulla creazione della posizione, vedereFornire DataSync l'accesso ai file server NFS.

DataSync sceglie automaticamente la versione NFS che utilizza per leggere da una posizione NFS. Per specificare una versione NFS, utilizzare il parametro opzionale `Version` nell'operazione API NfsMountOptions.

Questo comando restituisce l'Amazon Resource Name (ARN) della posizione NFS, simile a quello mostrato di seguito.

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

Per fare in modo che la directory possa essere montata, è possibile connettersi a qualsiasi computer che abbia la stessa configurazione di rete dell'agente ed eseguire il seguente comando.

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

Di seguito è riportato un comando di esempio.

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

Configurazione dei AWS DataSync trasferimenti con un file server SMB

Con AWS DataSync, è possibile trasferire dati tra il file server Server Message Block (SMB) e uno dei seguenti servizi di AWS storage:

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Per configurare questo tipo di trasferimento, devi creare una posizione per il tuo file server SMB. È possibile utilizzarlo come fonte o destinazione di trasferimento.

Fornire DataSync l'accesso ai file server SMB

DataSync si connette al file server utilizzando il protocollo SMB e può eseguire l'autenticazione con NTLM o Kerberos.

Argomenti

- Versioni SMB supportate
- Utilizzo dell'autenticazione NTLM
- Utilizzo di Autenticazione Kerberos

- Autorizzazioni richieste
- Namespace DFS

Versioni SMB supportate

Per impostazione predefinita, sceglie DataSync automaticamente una versione del protocollo SMB in base alla negoziazione con il file server SMB.

Puoi anche configurare l'utilizzo DataSync di una versione SMB specifica, ma ti consigliamo di farlo solo se hai problemi a negoziare automaticamente con DataSync il file server SMB. DataSync supporta le versioni SMB 1.0 e successive. Per motivi di sicurezza, consigliamo di utilizzare la versione 3.0.2 o successiva di SMB. Le versioni precedenti, come SMB 1.0, contengono vulnerabilità di sicurezza note che gli aggressori possono sfruttare per compromettere i dati.

Consulta la tabella seguente per un elenco delle opzioni disponibili nella console e nell'API: DataSync

Opzione Console	Opzione API	Descrizione
Automatica	`AUTOMATIC`	DataSync e il file server SMB negoziano la versione più recente di SMB che supportano reciprocamente tra la 2.1 e la 3.1.1. Questa è l'opzione predefinita e consigliata. Se scegli una versione specifica che il tuo server di file non supporta, potresti ricevere un errore `Operation Not Supported` .
SMB 3.0.2	`SMB3`	Limita la negoziazione del protocollo alla sola versione SMB 3.0.2.
SMB 2.1	`SMB2`	Limita la negoziazione del protocollo alla sola versione 2.1 di SMB.
SMB 2.0	`SMB2_0`	Limita la negoziazione del protocollo solo alla versione 2.0 di SMB.
SMB 1.0	`SMB1`	Limita la negoziazione del protocollo solo alla versione 1.0 di SMB.

Utilizzo dell'autenticazione NTLM

Per utilizzare l'autenticazione NTLM, devi fornire un nome utente e una password che consentano di accedere DataSync al file server SMB da cui stai effettuando il trasferimento. L'utente può essere un utente locale sul file server o un utente di dominio in Microsoft Active Directory.

Utilizzo di Autenticazione Kerberos

Per utilizzare l'autenticazione Kerberos, fornisci un principale Kerberos, un file di tabella delle chiavi Kerberos (keytab) e un file di configurazione Kerberos che consente di accedere DataSync al file server SMB da cui stai trasferendo o da cui stai effettuando il trasferimento.

Argomenti

- Prerequisiti
- DataSync opzioni di configurazione per Kerberos

Prerequisiti

È necessario creare un paio di artefatti Kerberos e configurare la rete in modo che possa accedere al file server SMB. DataSync

- Crea un file keytab Kerberos utilizzando l'utilità ktpass o kutil.

  L'esempio seguente crea un file keytab utilizzando. `ktpass` L'area di autenticazione Kerberos specificata (`MYDOMAIN.ORG`) deve essere in lettere maiuscole.

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

- Preparate una versione semplificata del file di configurazione Kerberos (). `krb5.conf` Includi informazioni sul realm, sulla posizione dei server di amministrazione del dominio e sulla mappatura dei nomi host su un realm Kerberos.

  Verifica che il `krb5.conf` contenuto sia formattato con l'involucro misto corretto per i nomi dei realm e dei nomi di dominio. Per esempio:

  ```
  [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
```

- Nella configurazione di rete, assicuratevi che la porta del server Kerberos Key Distribution Center (KDC) sia aperta. La porta KDC è in genere la porta TCP 88.

DataSync opzioni di configurazione per Kerberos

Quando si crea una sede SMB che utilizza Kerberos, si configurano le seguenti opzioni.

Opzione Console	Opzione API	Descrizione
Server SMB	`ServerHostName`	Il nome di dominio del file server SMB che verrà installat o dall' DataSyncagente. Per Kerberos, non è possibile specificare l'indirizzo IP del file server.
Principal di Kerberos	`KerberosPrincipal`	Un'identità nell'ambito Kerberos che dispone dell'auto rizzazione ad accedere a file, cartelle e metadati dei file nel file server SMB. Potrebbe essere simile a un principale Kerberos. `HOST/kerberosuser@MYDOMAIN.ORG`

Opzione Console	Opzione API	Descrizione
		I nomi principali distinguono tra maiuscole e minuscole.
File Keytab	`KerberosKeytab`	Un file di tabella delle chiavi Kerberos (keytab), che include le mappature tra la chiave principale Kerberos e la chiave di crittografia.
File di configurazione Kerberos	`KerberosKrbConf`	Un `krb5.conf` file che definisce la configurazione del realm Kerberos.
Indirizzi IP DNS (facoltativi)	`DnsIpAddresses`	Gli IPv4 indirizzi dei server DNS a cui appartiene il file server SMB. Se nel tuo ambiente sono presenti più domini, la configurazione garantisce la DataSync connessione al file server SMB corretto.

Autorizzazioni richieste

L'identità fornita DataSync deve disporre dell'autorizzazione per montare e accedere ai file, alle cartelle e ai metadati dei file del file server SMB.

Se fornisci un'identità in Active Directory, questa deve essere un membro di un gruppo Active Directory con uno o entrambi i seguenti diritti utente (a seconda dei metadati che desideri DataSync copiare):

Diritto dell'utente	Descrizione
Ripristinare file e directory () `SE_RESTORE_NAME`	Consente di DataSync copiare la proprietà degli oggetti, le autorizzazioni, i metadati dei file e

Diritto dell'utente	Descrizione
	gli elenchi di accesso discrezionali NTFS (). DACLs Questo diritto utente viene in genere concesso ai membri dei gruppi Domain Admins e Backup Operators (entrambi gruppi Active Directory predefiniti).
Gestisci i registri di controllo e sicurezza () `SE_SECURITY_NAME`	Consente di copiare DataSync gli elenchi di controllo degli accessi al sistema NTFS ()SACLs. Questo diritto utente viene generalmente concesso ai membri del gruppo Domain Admins.

Se desideri copiare Windows ACLs e stai effettuando un trasferimento tra un file server SMB e un altro sistema di storage che utilizza SMB (come Amazon FSx for Windows File Server o FSx ONTAP), l'identità fornita DataSync deve appartenere allo stesso dominio Active Directory o avere una relazione di trust Active Directory tra i rispettivi domini.

Namespace DFS

DataSync non supporta i namespace Microsoft Distributed File System (DFS). Ti consigliamo invece di specificare un file server o una condivisione sottostante quando crei la tua posizione. DataSync

Creazione della sede di trasferimento SMB

Prima di iniziare, è necessario un file server SMB da cui trasferire i dati.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per Location type (Tipo di posizione), scegliere Server Message Block (SMB).

Sarà possibile configurare questa posizione come origine o destinazione in un secondo momento.

4. Per gli agenti, scegli l' DataSync agente che può connettersi al tuo file server SMB.

   Puoi scegliere più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .

5. Per il server SMB, inserisci il nome di dominio o l'indirizzo IP del file server SMB che verrà installato dall' DataSync agente.

   Ricorda quanto segue con questa impostazione:

   - Non puoi specificare un indirizzo IP versione 6 (IPv6).
   - Se utilizzi l'autenticazione Kerberos, devi specificare un nome di dominio.

6. Per Share name, inserisci il nome della condivisione esportata dal tuo file server SMB dove DataSync leggerà o scriverà i dati.

   È possibile includere una sottodirectory nel percorso di condivisione (ad esempio,). `/path/to/subdirectory` Assicurati che anche altri client SMB della tua rete possano montare questo percorso.

   Per copiare tutti i dati nella sottodirectory, DataSync devi essere in grado di montare la condivisione SMB e accedere a tutti i suoi dati. Per ulteriori informazioni, consulta Autorizzazioni richieste.

7. (Facoltativo) Espandi le impostazioni aggiuntive e scegli una versione SMB DataSync da utilizzare per accedere al file server.

   Per impostazione predefinita, sceglie DataSync automaticamente una versione in base alla negoziazione con il file server SMB. Per informazioni, consultare Versioni SMB supportate.

8. Per il tipo di autenticazione, scegli NTLM o Kerberos.

9. Effettua una delle seguenti operazioni a seconda del tipo di autenticazione:

   NTLM

   - Per Utente, inserisci un nome utente che possa montare il file server SMB e che disponga dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.

     Per ulteriori informazioni, consulta Autorizzazioni richieste.

- Per Password, inserisci la password dell'utente che può installare il file server SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.
- (Facoltativo) In Dominio, inserite il nome di dominio Windows a cui appartiene il file server SMB.

  Se nel tuo ambiente sono presenti più domini, la configurazione di questa impostazione assicura che DataSync si connetta al file server SMB corretto.

Kerberos

- Per il principale Kerberos, specifica un principale nel tuo realm Kerberos che disponga dell'autorizzazione ad accedere ai file, alle cartelle e ai metadati dei file nel tuo file server SMB.

  Potrebbe essere simile a un principale Kerberos. `HOST/kerberosuser@MYDOMAIN.ORG`

  I nomi principali distinguono tra maiuscole e minuscole. L'esecuzione dell' DataSyncattività avrà esito negativo se il principale specificato per questa impostazione non corrisponde esattamente al principale utilizzato per creare il file keytab.
- Per il file Keytab, carica un file keytab che includa le mappature tra la chiave principale Kerberos e la chiave di crittografia.
- Per il file di configurazione Kerberos, carica un **`krb5.conf`** file che definisca la configurazione del tuo realm Kerberos.
- (Facoltativo) Per gli indirizzi IP DNS, specifica fino a due IPv4 indirizzi per i server DNS a cui appartiene il file server SMB.

  Se nel tuo ambiente sono presenti più domini, la configurazione di questo parametro assicura che DataSync si connetta al file server SMB corretto.

10. (Facoltativo) Scegli Aggiungi tag per etichettare la tua posizione SMB.

    I tag sono coppie chiave-valore che ti aiutano a gestire, filtrare e cercare le tue sedi. È consigliabile creare almeno un tag di nome per la posizione.
11. Scegli Crea località.

Usando il AWS CLI

Le seguenti istruzioni descrivono come creare sedi SMB con autenticazione NTLM o Kerberos.

NTLM

1. Copia il comando seguente. `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. Per`--agent-arns`, specifica l' DataSync agente che può connettersi al file server SMB.

   Puoi scegliere più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .

3. Per`--server-hostname`, specifica il nome di dominio o l' IPv4 indirizzo del file server SMB che verrà installato dall' DataSync agente.

4. Ad `--subdirectory` esempio, specifica il nome della condivisione esportata dal file server SMB in cui DataSync leggerà o scriverà i dati.

   È possibile includere una sottodirectory nel percorso di condivisione (ad esempio,). `/path/to/subdirectory` Assicurati che anche altri client SMB della tua rete possano montare questo percorso.

   Per copiare tutti i dati nella sottodirectory, DataSync devi essere in grado di montare la condivisione SMB e accedere a tutti i suoi dati. Per ulteriori informazioni, consulta Autorizzazioni richieste.

5. Ad `--user` esempio, specifica un nome utente in grado di montare il file server SMB e che disponga dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.

   Per ulteriori informazioni, consulta Autorizzazioni richieste.

6. Ad `--password` esempio, specifica la password dell'utente che può installare il file server SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.

7. (Facoltativo) Per`--domain`, specifica il nome di dominio Windows a cui appartiene il file server SMB.

Se nel tuo ambiente sono presenti più domini, la configurazione di questa impostazione assicura che DataSync si connetta al file server SMB corretto.

8. (Facoltativo) Aggiungi l'`--version`opzione se desideri DataSync utilizzare una versione SMB specifica. Per ulteriori informazioni, consulta Versioni SMB supportate.
9. Esegui il comando `create-location-smb`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN della posizione creata. Per esempio:

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

Kerberos

1. Copia il seguente `create-location-smb` comando.

   ```
   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 "fileb://path/to/file.keytab" \
       --kerberos-krb5-conf "file://path/to/krb5.conf" \
       --dns-ip-addresses array-of-ipv4-addresses
   ```

2. Per`--agent-arns`, specifica l' DataSync agente che può connettersi al file server SMB.

   Puoi scegliere più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .
3. Per`--server-hostname`, specifica il nome di dominio del file server SMB che il tuo DataSync agente installerà.
4. Ad `--subdirectory` esempio, specifica il nome della condivisione esportata dal file server SMB in cui DataSync leggerà o scriverà i dati.

È possibile includere una sottodirectory nel percorso di condivisione (ad esempio,). `/path/to/subdirectory` Assicurati che anche altri client SMB della tua rete possano montare questo percorso.

Per copiare tutti i dati nella sottodirectory, DataSync devi essere in grado di montare la condivisione SMB e accedere a tutti i suoi dati. Per ulteriori informazioni, consulta Autorizzazioni richieste.

5. Per le opzioni Kerberos, effettuate le seguenti operazioni:

   - `--kerberos-principal`: Specificate un principale nel vostro realm Kerberos che disponga dell'autorizzazione ad accedere ai file, alle cartelle e ai metadati dei file nel file server SMB.

     Potrebbe essere simile a un principale Kerberos. `HOST/kerberosuser@MYDOMAIN.ORG`

     I nomi principali distinguono tra maiuscole e minuscole. L'esecuzione dell' DataSyncattività avrà esito negativo se il principale specificato per questa opzione non corrisponde esattamente al principale utilizzato per creare il file keytab.
   - `--kerberos-keytab`: Specificate un file keytab che includa le mappature tra il principale Kerberos e le chiavi di crittografia.
   - `--kerberos-krb5-conf`: Specificate un `krb5.conf` file che definisce la configurazione del realm Kerberos.
   - (Facoltativo)`--dns-ip-addresses`: Specificate fino a due IPv4 indirizzi per i server DNS a cui appartiene il file server SMB.

     Se nel tuo ambiente sono presenti più domini, la configurazione di questo parametro assicura che DataSync si connetta al file server SMB corretto.
6. (Facoltativo) Aggiungi l'`--version`opzione se desideri DataSync utilizzare una versione SMB specifica. Per ulteriori informazioni, consulta Versioni SMB supportate.
7. Esegui il comando `create-location-smb`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN della posizione creata. Per esempio:

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

Configurazione dei AWS DataSync trasferimenti con un cluster HDFS

Con AWS DataSync, è possibile trasferire dati tra il cluster Hadoop Distributed File System (HDFS) e uno dei seguenti servizi di archiviazione: AWS

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Per configurare questo tipo di trasferimento, crei una posizione per il tuo cluster HDFS. È possibile utilizzare questa posizione come fonte o destinazione di trasferimento.

Fornire DataSync l'accesso ai cluster HDFS

Per connettersi al cluster HDFS, DataSync utilizza un agente distribuito il più vicino possibile al cluster HDFS. L' DataSyncagente funge da client HDFS e comunica con e all'interno del NameNodes cluster. DataNodes

Quando si avvia un'operazione di trasferimento, DataSync interroga NameNode le posizioni dei file e delle cartelle nel cluster. Se configuri la posizione HDFS come posizione di origine, DataSync legge i file e i dati delle cartelle dal cluster e li copia DataNodes nella destinazione. Se configuri la posizione HDFS come posizione di destinazione, DataSync scrive file e cartelle dall'origine a quella del cluster DataNodes .

Autenticazione

Quando ci si connette a un cluster HDFS, DataSync supporta l'autenticazione semplice o l'autenticazione Kerberos. Per utilizzare l'autenticazione semplice, fornisci il nome utente di un utente con i diritti di lettura e scrittura sul cluster HDFS. Per utilizzare l'autenticazione Kerberos, fornite un file di configurazione Kerberos, un file della tabella delle chiavi Kerberos (keytab) e un nome principale Kerberos. Le credenziali del principale Kerberos devono trovarsi nel file keytab fornito.

Crittografia

Quando si utilizza l'autenticazione Kerberos, DataSync supporta la crittografia dei dati durante la trasmissione tra l'agente e il DataSync cluster HDFS. Crittografa i dati utilizzando le impostazioni di

configurazione Quality of Protection (QOP) sul cluster HDFS e specificando le impostazioni QOP durante la creazione della posizione HDFS. La configurazione QOP include le impostazioni per la protezione del trasferimento dei dati e la protezione RPC (Remote Procedure Call).

DataSync supporta i seguenti tipi di crittografia Kerberos:

- `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`

È inoltre possibile configurare i cluster HDFS per la crittografia inattiva utilizzando Transparent Data Encryption (TDE). Quando si utilizza l'autenticazione semplice, DataSync legge e scrive su cluster compatibili con TDE. Se usi DataSync per copiare i dati su un cluster abilitato per TDE, configura innanzitutto le zone di crittografia sul cluster HDFS. DataSync non crea zone di crittografia.

Funzionalità HDFS non supportate

Le seguenti funzionalità HDFS non sono attualmente supportate da: DataSync

- Transparent Data Encryption (TDE) quando si utilizza l'autenticazione Kerberos
- Configurazione multipla NameNodes
- Hadoop HDFS su HTTP (HttpFS)
- Liste di controllo degli accessi POSIX () ACLs
- Attributi estesi HDFS (xattrs)
- Cluster HDFS che utilizzano Apache HBase

Creazione della posizione di trasferimento HDFS

Puoi usare la tua posizione come origine o destinazione per il DataSync trasferimento.

Prima di iniziare: verifica la connettività di rete tra l'agente e il cluster Hadoop effettuando le seguenti operazioni:

- Verifica l'accesso alle porte TCP elencate in. Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge
- Verifica l'accesso tra l'agente locale e il cluster Hadoop. Per istruzioni, consultare Verifica della connessione dell'agente al sistema di storage.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo. https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per il tipo di posizione, scegli Hadoop Distributed File System (HDFS).

   Puoi configurare questa posizione come origine o destinazione in un secondo momento.
4. Per gli agenti, scegli l'agente che può connettersi al tuo cluster HDFS.

   Puoi scegliere più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .
5. Per NameNode, fornisci il nome di dominio o l'indirizzo IP del principale NameNode del cluster HDFS.
6. Per Cartella, inserisci una cartella sul cluster HDFS che desideri utilizzare DataSync per il trasferimento dei dati.

   Se la posizione HDFS è un'origine, DataSync copia i file in questa cartella nella destinazione. Se la tua posizione è una destinazione, DataSync scrive i file in questa cartella.
7. Per impostare la dimensione del blocco o il fattore di replica, scegli Impostazioni aggiuntive.

   La dimensione predefinita del blocco è 128 MiB. Le dimensioni dei blocchi fornite devono essere un multiplo di 512 byte.

   Il fattore di replica predefinito è tre DataNodes durante il trasferimento al cluster HDFS.

8. Nella sezione Sicurezza, scegli il tipo di autenticazione utilizzato sul tuo cluster HDFS.

   - Semplice: per Utente, specifica il nome utente con le seguenti autorizzazioni sul cluster HDFS (a seconda del caso d'uso):
     - Se intendi utilizzare questa posizione come posizione di origine, specifica un utente con solo autorizzazioni di lettura.
     - Se intendi utilizzare questa posizione come posizione di destinazione, specifica un utente con autorizzazioni di lettura e scrittura.

     Facoltativamente, specifica l'URI del Key Management Server (KMS) del cluster HDFS.
   - Kerberos: specifica il Kerberos Principal con accesso al cluster HDFS. Quindi, fornisci il KeyTabfile che contiene il principale Kerberos fornito. Fornite quindi il file di configurazione Kerberos. Infine, specifica il tipo di crittografia nella protezione del transito negli elenchi a discesa Protezione RPC e Protezione trasferimento dati.
9. (Facoltativo) Scegli Aggiungi tag per etichettare la tua posizione HDFS.

   I tag sono coppie chiave-valore che ti aiutano a gestire, filtrare e cercare le tue sedi. È consigliabile creare almeno un tag di nome per la posizione.
10. Scegli Crea località.

Usando il AWS CLI

1. Copia il seguente `create-location-hdfs` comando.

```
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. Per il `--name-nodes` parametro, specifica il nome host o l'indirizzo IP del principale del cluster HDFS NameNode e la porta TCP su cui NameNode è in ascolto.
3. Per il `--authentication-type` parametro, specifica il tipo di autenticazione da utilizzare per la connessione al cluster Hadoop. Puoi specificare `SIMPLE` o `KERBEROS`.

   Se si utilizza `SIMPLE` l'autenticazione, utilizzare il `--simple-user` parametro per specificare il nome utente dell'utente. Se si utilizza `KERBEROS` l'autenticazione, utilizzare i `--kerberos-`

`principal` `--kerberos-krb5-conf` parametri`--kerberos-keytab`, and. Per ulteriori informazioni, consulta create-location-hdfs.

4. Per il `--agent-arns` parametro, specifica l'ARN dell' DataSync agente che può connettersi al cluster HDFS.

   Puoi scegliere più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .

5. (Facoltativo) Per il `--subdirectory` parametro, specifica una cartella sul cluster HDFS che desideri utilizzare DataSync per il trasferimento dei dati.

   Se la posizione HDFS è un'origine, DataSync copia i file in questa cartella nella destinazione. Se la tua posizione è una destinazione, DataSync scrive i file in questa cartella.

6. Esegui il comando `create-location-hdfs`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN della posizione creata. Per esempio:

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

Configurazione dei DataSync trasferimenti con un sistema di archiviazione di oggetti

Con AWS DataSync, è possibile trasferire dati tra il sistema di storage degli oggetti e uno dei seguenti servizi di AWS storage:

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Per configurare questo tipo di trasferimento, crei una posizione per il tuo sistema di storage di oggetti. È possibile utilizzare questa posizione come origine o destinazione di trasferimento. Il trasferimento di dati da o verso lo storage di oggetti locale richiede un DataSync agente.

Prerequisiti

Il tuo sistema di storage a oggetti deve essere compatibile con le seguenti operazioni dell'API Amazon S3 per DataSync poterti connettere:

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

Creazione della posizione di trasferimento dello storage degli oggetti

Prima di iniziare, è necessario un sistema di storage di oggetti verso o da cui trasferire i dati.

Utilizzo della console di DataSync

1. Aprire la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.

3. Per Tipo di posizione, scegli Archiviazione oggetti.

   Sarà possibile configurare questa posizione come origine o destinazione in un secondo momento.

4. Per Server, fornisci il nome di dominio o l'indirizzo IP del server di archiviazione degli oggetti.

5. Per Bucket name, inserisci il nome del bucket di archiviazione degli oggetti coinvolto nel trasferimento.

6. Per Folder, immettete il prefisso dell'oggetto.

   DataSync copia solo gli oggetti con questo prefisso.

7. Se il trasferimento richiede un agente, scegli Usa agenti, quindi scegli l' DataSync agente che si connette al tuo sistema di storage degli oggetti.

   Alcuni trasferimenti non richiedono agenti. In altri scenari, potresti voler utilizzare più di un agente. Per ulteriori informazioni, consultare Situazioni in cui non è necessario un agente DataSync e Utilizzo di più agenti DataSync .

8. Per configurare la connessione al server di archiviazione degli oggetti, espandi Impostazioni aggiuntive ed esegui le seguenti operazioni:

   a. Per il protocollo Server, scegli HTTP o HTTPS.

   b. Per Porta server, usa una porta predefinita (80 per HTTP o 443 per HTTPS) o specifica una porta personalizzata, se necessario.

   c. Per Certificato, se il sistema di archiviazione degli oggetti utilizza un'autorità di certificazione (CA) privata o autofirmata, seleziona Scegli file e specifica un singolo `.pem` file con una catena di certificati completa.

      La catena di certificati potrebbe includere:

      - Il certificato del sistema di archiviazione degli oggetti
      - Tutti i certificati intermedi (se presenti)
      - Il certificato principale della CA firmataria

      È possibile concatenare i certificati in un `.pem` file (che può contenere fino a 32768 byte prima della codifica in base64). Il `cat` comando di esempio seguente crea un file che include tre certificati: *`object_storage_certificates`*`.pem`

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

9. Se il server di archiviazione degli oggetti richiede credenziali per l'accesso, seleziona Richiede credenziali e inserisci la chiave di accesso che usi per accedere al bucket. Quindi inserisci direttamente la chiave segreta o specifica un AWS Secrets Manager segreto che contenga la chiave. Per ulteriori informazioni, vedere Fornitura di credenziali per le posizioni di archiviazione.

   La chiave di accesso e la chiave segreta possono essere rispettivamente un nome utente e una password.

10. (Facoltativo) Scegliete Aggiungi tag per etichettare la posizione di archiviazione degli oggetti.

    I tag sono coppie chiave-valore che ti aiutano a gestire, filtrare e cercare le tue posizioni. È consigliabile creare almeno un tag di nome per la posizione.

11. Scegli Crea località.

Usando il AWS CLI

1. Copia il seguente `create-location-object-storage` comando:

```
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. Specificate i seguenti parametri obbligatori nel comando:

   - `--server-hostname`— Specificare il nome di dominio o l'indirizzo IP del server di archiviazione degli oggetti.
   - `--bucket-name`— Specificate il nome del bucket sul server di archiviazione degli oggetti su cui state trasferendo o da cui state effettuando il trasferimento.

3. (Facoltativo) Aggiungi uno dei seguenti parametri al comando:

   - `--agent-arns`— Specificare gli DataSync agenti che si desidera connettere al server di archiviazione degli oggetti.
   - `--server-port`— Speciifica la porta su cui il server di archiviazione degli oggetti accetta il traffico di rete in entrata (ad esempio, la porta`443`).

- `--server-protocol`— Speciifica il protocollo (HTTPoHTTPS) utilizzato dal server di archiviazione degli oggetti per comunicare.
- `--access-key`— Speciifica la chiave di accesso (ad esempio, un nome utente) se sono necessarie credenziali per l'autenticazione con il server di archiviazione degli oggetti.
- `--secret-key`— Speciifica la chiave segreta (ad esempio una password) se sono necessarie credenziali per l'autenticazione con il server di archiviazione degli oggetti.

  È inoltre possibile fornire parametri aggiuntivi per proteggere le chiavi utilizzando. AWS Secrets Manager Per ulteriori informazioni, vedere Fornitura di credenziali per le posizioni di archiviazione.
- `--server-certificate`— Speciifica una catena di certificati DataSync per l'autenticazione con il sistema di storage di oggetti se il sistema utilizza un'autorità di certificazione (CA) privata o autofirmata. È necessario specificare un singolo `.pem` file con una catena di certificati completa (ad esempio,). `file:///home/user/.ssh/object_storage_certificates.pem`

  La catena di certificati potrebbe includere:

  - Il certificato del sistema di archiviazione degli oggetti
  - Tutti i certificati intermedi (se presenti)
  - Il certificato principale della CA firmataria

  È possibile concatenare i certificati in un `.pem` file (che può contenere fino a 32768 byte prima della codifica in base64). Il `cat` comando di esempio seguente crea un file che include tre certificati: *`object_storage_certificates`*`.pem`

  ```
  cat object_server_certificate.pem intermediate_certificate.pem ca_root_certificate.pem
   > object_storage_certificates.pem
  ```
- `--subdirectory`— specifica il prefisso dell'oggetto per il server di archiviazione degli oggetti.

  DataSync copia solo gli oggetti con questo prefisso.
- `--tags`— specifica la coppia chiave-valore che rappresenta un tag da aggiungere alla risorsa di localizzazione.

  I tag ti aiutano a gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.

4. Esegui il comando `create-location-object-storage`.

   Riceverai una risposta che ti mostra l'ARN della posizione che hai appena creato.

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

Trasferimento da o verso AWS lo storage con AWS DataSync

Con AWS DataSync, puoi trasferire dati da o verso una serie di servizi di AWS archiviazione. Per ulteriori informazioni, vedi Con dove posso trasferire i miei dati DataSync?

Argomenti

- Configurazione dei AWS DataSync trasferimenti con Amazon S3
- Configurazione dei AWS DataSync trasferimenti con Amazon EFS
- Configurazione dei trasferimenti con FSx per Windows File Server
- Configurazione dei DataSync trasferimenti con FSx for Lustre
- Configurazione dei DataSync trasferimenti con Amazon FSx per OpenZFS
- Configurazione dei trasferimenti con Amazon FSx for NetApp ONTAP

Configurazione dei AWS DataSync trasferimenti con Amazon S3

Per trasferire dati da o verso il tuo bucket Amazon S3, devi creare una AWS DataSync posizione di trasferimento. DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Fornire DataSync l'accesso ai bucket S3

DataSync ha bisogno di accedere al bucket S3 verso o da cui stai trasferendo. Per fare ciò, devi creare un ruolo AWS Identity and Access Management (IAM) che DataSync presupponga le autorizzazioni necessarie per accedere al bucket. Specificate quindi questo ruolo quando create la vostra sede Amazon S3 per. DataSync

Indice

- Autorizzazioni richieste
- Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3
- Accesso ai bucket S3 utilizzando la crittografia lato server
- Accesso a bucket S3 con restrizioni
- Accesso ai bucket S3 con accesso VPC limitato

Autorizzazioni richieste

Le autorizzazioni richieste dal tuo ruolo IAM possono dipendere dal fatto che il bucket sia una posizione di DataSync origine o di destinazione. Amazon S3 on Outposts richiede un set di autorizzazioni diverso.

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:AbortMultipartUpload",
                "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"
```

```
        }
    ]
}
```

Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3

Quando crei la tua posizione Amazon S3 nella console, DataSync puoi creare e assumere automaticamente un ruolo IAM che normalmente dispone delle autorizzazioni giuste per accedere al tuo bucket S3.

In alcune situazioni, potrebbe essere necessario creare questo ruolo manualmente (ad esempio, accedere a bucket con livelli di sicurezza aggiuntivi o trasferire da o verso un bucket in un altro). Account AWS

Creazione manuale di un ruolo IAM per DataSync

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli, quindi scegli Crea ruolo.
3. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli Servizio AWS.
4. Per Caso d'uso, scegli DataSyncnell'elenco a discesa e seleziona DataSync. Scegli Next (Successivo).
5. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo). Dai un nome al tuo ruolo e scegli Crea ruolo.
6. Nella pagina Ruoli, cerca il ruolo che hai appena creato e scegline il nome.
7. Nella pagina dei dettagli del ruolo, scegli la scheda Autorizzazioni. Scegli Aggiungi autorizzazioni, quindi Crea politica in linea.
8. Scegli la scheda JSON e aggiungi le autorizzazioni necessarie per accedere al tuo bucket nell'editor delle politiche.
9. Scegli Next (Successivo). Dai un nome alla tua politica e scegli Crea politica.
10. (Consigliato) Per evitare il problema del sostituto confuso tra diversi servizi, procedi come segue:

    a. Nella pagina dei dettagli del ruolo, scegli la scheda Relazioni di fiducia. Seleziona Modifica policy di attendibilità.

    b. Aggiorna la politica di fiducia utilizzando l'esempio seguente, che include le chiavi del contesto `aws:SourceArn` e della condizione `aws:SourceAccount` globale:

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. Scegli Aggiorna policy.

Puoi specificare questo ruolo durante la creazione della tua sede Amazon S3.

Accesso ai bucket S3 utilizzando la crittografia lato server

DataSync può trasferire dati da o verso i bucket S3 che utilizzano la crittografia lato server. Il tipo di chiave di crittografia utilizzata da un bucket può determinare se è necessaria una politica personalizzata che DataSync consenta di accedere al bucket.

Quando lo utilizzi DataSync con bucket S3 che utilizzano la crittografia lato server, ricorda quanto segue:

- Se il tuo bucket S3 è crittografato con una chiave AWS gestita, DataSync puoi accedere agli oggetti del bucket per impostazione predefinita se tutte le tue risorse sono nelle stesse. Account AWS

- Se il bucket S3 è crittografato con una chiave gestita dal cliente AWS Key Management Service (AWS KMS) (SSE-KMS), la policy della chiave deve includere il ruolo IAM utilizzato per accedere al bucket. DataSync
- Se il bucket S3 è crittografato con una chiave SSE-KMS gestita dal cliente e in un'altra chiave, è necessaria l'autorizzazione per accedere al bucket dell'altro Account AWS. DataSync Account AWS Puoi configurarlo effettuando le seguenti operazioni:
  - Nel ruolo IAM DataSync utilizzato, devi specificare la chiave SSE-KMS del bucket cross-account utilizzando l'Amazon Resource Name (ARN) completo della chiave. Questa è la stessa chiave ARN che usi per configurare la crittografia predefinita del bucket. In questa situazione non è possibile specificare un ID chiave, un nome alias o un alias ARN.

    Ecco un esempio di codice ARN:

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

    Per ulteriori informazioni sulla specificazione delle chiavi KMS nelle dichiarazioni politiche IAM, consulta la AWS Key Management Service Developer Guide.
  - Nella policy chiave SSE-KMS, specifica il ruolo IAM utilizzato da. DataSync
- Se il bucket S3 è crittografato con una AWS KMS chiave gestita dal cliente (DSSE-KMS) per la crittografia lato server a doppio livello, la policy della chiave deve includere il ruolo IAM utilizzato per accedere al bucket. DataSync (Tieni presente che DSSE-KMS non supporta S3 Bucket Keys, il che può ridurre i costi delle richieste.) AWS KMS
- Se il tuo bucket S3 è crittografato con una chiave di crittografia fornita dal cliente (SSE-C), non puoi accedere a questo bucket. DataSync

Esempio: politica chiave SSE-KMS per DataSync

L'esempio seguente è una politica chiave per una chiave SSE-KMS gestita dal cliente. La policy è associata a un bucket S3 che utilizza la crittografia lato server.

Se desideri utilizzare questo esempio, sostituisci i seguenti valori con i tuoi:

- *`account-id`*— Il tuo Account AWS.
- *`admin-role-name`*— Il nome del ruolo IAM che può amministrare la chiave.
- *`datasync-role-name`*— Il nome del ruolo IAM che consente di DataSync utilizzare la chiave per accedere al bucket.

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": "*"
        }
    ]
}
```

Accesso a bucket S3 con restrizioni

Se devi trasferire da o verso un bucket S3 che in genere nega ogni accesso, puoi modificare la policy del bucket in modo che DataSync possa accedere al bucket solo per il trasferimento.

Esempio: consentire l'accesso in base ai ruoli IAM

1. Copia la seguente policy sui bucket S3.

   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. Nella politica, sostituisci i seguenti valori:

   - *amzn-s3-demo-bucket*— Specificare il nome del bucket S3 con restrizioni.
   - *datasync-iam-role-id*— Specificare l'ID del ruolo IAM DataSync utilizzato per accedere al bucket.

     Esegui il AWS CLI comando seguente per ottenere l'ID del ruolo IAM:

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

     Nell'output, cerca il `RoleId` valore:

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

   - *your-iam-role-id*— Specificate l'ID del ruolo IAM che utilizzate per creare la vostra DataSync posizione per il bucket.

     Esegui il comando seguente per ottenere l'ID del ruolo IAM:

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

     Nell'output, cerca il `RoleId` valore:

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

3. Aggiungi questa policy alla tua policy sui bucket S3.
4. Quando hai finito di utilizzare il bucket DataSync con restrizioni, rimuovi le condizioni per entrambi i ruoli IAM dalla policy del bucket.

Accesso ai bucket S3 con accesso VPC limitato

Un bucket Amazon S3 che limita l'accesso a specifici endpoint del cloud privato virtuale (VPC) o che nega il trasferimento DataSync da o VPCs verso quel bucket. Per abilitare i trasferimenti in queste situazioni, puoi aggiornare la policy del bucket per includere il ruolo IAM che specifichi con la tua posizione. DataSync

Option 1: Allowing access based on DataSync location role ARN

Nella policy del bucket S3, puoi specificare l'Amazon Resource Name (ARN) del ruolo IAM della tua DataSync posizione.

L'esempio seguente è una policy sui bucket S3 che nega l'accesso a tutti tranne due (e). VPCs `vpc-1234567890abcdef0` `vpc-abcdef01234567890` Tuttavia, la policy include anche ArnNotLikeIfExistscondition e aws: PrincipalArn condition key, che consentono all'ARN di un ruolo di DataSync location di accedere al bucket.

```
{
    "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

Nella policy del bucket S3, puoi specificare un tag allegato al tuo DataSync ruolo IAM di location.

L'esempio seguente è una policy sui bucket S3 che nega l'accesso a tutti tranne due (e). VPCs `vpc-1234567890abcdef0` `vpc-abcdef01234567890` Tuttavia, la policy include anche StringNotEqualsIfExistscondition e aws: PrincipalTag condition key, che consentono un principal con la chiave `exclude-from-vpc-restriction` e il valore del tag. `true` Puoi provare un approccio simile nella tua policy sui bucket specificando un tag associato al tuo ruolo di DataSync location.

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

Considerazioni sulla classe di storage con Amazon S3 Transfers

Quando Amazon S3 è la tua posizione di destinazione, DataSync puoi trasferire i dati direttamente in una classe di storage Amazon S3 specifica.

Alcune classi di storage hanno comportamenti che possono influire sui costi di storage di Amazon S3. Quando si utilizzano classi di storage che possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione o il recupero di oggetti, le modifiche ai dati o ai metadati degli oggetti comportano tali costi. Per ulteriori informazioni, consulta Prezzi di Amazon S3.

Important

I nuovi oggetti trasferiti nella posizione di destinazione di Amazon S3 vengono archiviati utilizzando la classe di storage specificata durante la creazione della posizione.
Per impostazione predefinita, DataSync conserva la classe di storage degli oggetti esistenti nella posizione di destinazione, a meno che non configuri l'attività per trasferire tutti i dati. In tali situazioni, la classe di archiviazione specificata durante la creazione della posizione viene utilizzata per tutti gli oggetti.

Classe di storage Amazon S3	Considerazioni
S3 Standard	Scegli S3 Standard per archiviare i file a cui accedi di frequente in modo ridondante in più zone di disponibilità geograficamente separate. Questa è l'impostazione predefinita se non specifichi una classe di storage.
S3 Intelligent-Tiering	Scegli S3 Intelligent-Tiering per ottimizzare i costi di storage spostando automaticamente i dati nel livello di accesso allo storage più convenien te. Paghi una tariffa mensile per oggetto archiviato nella classe di storage S3 Intelligent-Tiering. Questa tariffa di Amazon S3 include il monitorag gio dei modelli di accesso ai dati e lo spostamento di oggetti tra livelli.
S3 Standard-IA	Scegli S3 Standard-IA per archiviare in modo ridondante gli oggetti a cui si accede raramente in più zone di disponibilità geograficamente separate. Gli oggetti archiviati nella classe di storage S3 Standard-IA possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione o il recupero. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessari o accedervi. Le modifiche ai dati o ai metadati degli oggetti equivalgono all'eliminazione di un oggetto e alla creazione di uno nuovo per sostituir lo. Ciò comporta costi aggiuntivi per gli oggetti archiviati nella classe di storage S3 Standard-IA.

Classe di storage Amazon S3	Considerazioni
	Gli oggetti inferiori a 128 KB sono inferiori al costo minimo di capacità per oggetto nella classe di storage S3 Standard-IA. Questi oggetti sono archiviati nella classe di storage S3 Standard.
S3 One Zone-IA	Scegli S3 One Zone-IA per archiviare gli oggetti a cui si accede raramente in un'unica zona di disponibilità. Gli oggetti archiviati nella classe di storage S3 One Zone-IA possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione o il recupero. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessari o accedervi. Le modifiche ai dati o ai metadati degli oggetti equivalgono all'eliminazione di un oggetto e alla creazione di uno nuovo per sostituir lo. Ciò comporta costi aggiuntivi per gli oggetti archiviati nella classe di storage S3 One Zone-IA. Gli oggetti inferiori a 128 KB sono inferiori al costo minimo di capacità per oggetto nella classe di storage S3 One Zone-IA. Questi oggetti sono archiviati nella classe di storage S3 Standard.

Classe di storage Amazon S3	Considerazioni
S3 Glacier Instant Retrieval	Scegli S3 Glacier Instant Retrieval per archiviare oggetti a cui si accede raramente ma che richiedono il recupero in millisecondi. I dati archiviati nella classe di storage S3 Glacier Instant Retrieval offrono risparmi sui costi rispetto alla classe di storage S3 Standard-IA con le stesse prestazioni di latenza e throughput. Tuttavia, S3 Glacier Instant Retrieval ha costi di accesso ai dati più elevati rispetto a S3 Standard-IA. Gli oggetti archiviati in S3 Glacier Instant Retrieval possono comportar e costi aggiuntivi per la sovrascrittura, l'eliminazione o il recupero. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Le modifiche ai dati o ai metadati degli oggetti equivalgono all'eliminazione di un oggetto e alla creazione di uno nuovo per sostituir lo. Ciò comporta costi aggiuntivi per gli oggetti archiviati nella classe di storage S3 Glacier Instant Retrieval. Gli oggetti inferiori a 128 KB sono inferiori al costo minimo di capacità per oggetto nella classe di storage S3 Glacier Instant Retrieval. Questi oggetti sono archiviati nella classe di storage S3 Standard.

Classe di storage Amazon S3	Considerazioni
S3 Glacier Flexible Retrieval	Scegli S3 Glacier Flexible Retrieval per archivi più attivi. Gli oggetti archiviati in S3 Glacier Flexible Retrieval possono comportar e costi aggiuntivi per la sovrascrittura, l'eliminazione o il recupero. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Le modifiche ai dati o ai metadati degli oggetti equivalgono all'eliminazione di un oggetto e alla creazione di uno nuovo per sostituir lo. Ciò comporta costi aggiuntivi per gli oggetti archiviati nella classe di storage S3 Glacier Flexible Retrieval. La classe di storage S3 Glacier Flexible Retrieval richiede 40 KB di metadati aggiuntivi per ogni oggetto archiviato. DataSync inserisce oggetti di dimensioni inferiori a 40 KB nella classe di storage S3 Standard. È necessario ripristinare gli oggetti archiviati in questa classe di archiviaz ione prima di DataSync poterli leggere. Per informazioni, consulta Lavorare con oggetti archiviati nella Guida per l'utente di Amazon S3. Quando usi S3 Glacier Flexible Retrieval, scegli l'opzione Verifica solo l'operazione di verifica dei dati trasferiti per confrontare i checksum di dati e metadati al termine del trasferimento. Non è possibile utilizzar e l'opzione Verifica tutti i dati nella destinazione per questa classe di archiviazione perché richiede il recupero di tutti gli oggetti esistenti dalla destinazione.

Classe di storage Amazon S3	Considerazioni
S3 Glacier Deep Archive	Scegli S3 Glacier Deep Archive per archiviare i tuoi oggetti per la conservazione dei dati a lungo termine e la conservazione digitale, laddove i dati siano accessibili una o due volte all'anno. Gli oggetti archiviati in S3 Glacier Deep Archive possono comportar e costi aggiuntivi per la sovrascrittura, l'eliminazione o il recupero. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Le modifiche ai dati o ai metadati degli oggetti equivalgono all'eliminazione di un oggetto e alla creazione di uno nuovo per sostituir lo. Ciò comporta costi aggiuntivi per gli oggetti archiviati nella classe di storage S3 Glacier Deep Archive. La classe di storage S3 Glacier Deep Archive richiede 40 KB di metadati aggiuntivi per ogni oggetto archiviato. DataSync inserisce gli oggetti che pesano meno di 40 KB nella classe di storage S3 Standard. È necessario ripristinare gli oggetti archiviati in questa classe di archiviaz ione prima di DataSync poterli leggere. Per informazioni, consulta Lavorare con oggetti archiviati nella Guida per l'utente di Amazon S3. Quando usi S3 Glacier Deep Archive, scegli l'opzione Verifica solo l'operazione di trasferimento dei dati per confrontare i checksum di dati e metadati al termine del trasferimento. Non è possibile utilizzare l'opzione Verifica tutti i dati nella destinazione per questa classe di archiviazione perché richiede il recupero di tutti gli oggetti esistenti dalla destinazione.
S3 Outposts	La classe di storage per Amazon S3 on Outposts.

Valutazione dei costi delle richieste S3 durante l'utilizzo DataSync

Con le sedi Amazon S3, devi sostenere i costi relativi alle richieste API S3 effettuate da. DataSync Questa sezione può aiutarti a capire come DataSync utilizza queste richieste e come potrebbero influire sui costi di Amazon S3.

Argomenti

- Richieste S3 effettuate da DataSync
- Considerazioni sui costi

Richieste S3 effettuate da DataSync

La tabella seguente descrive le richieste S3 che DataSync puoi effettuare quando copi dati da o verso una posizione Amazon S3.

Richiesta S3	Come DataSync lo usa
ListObjectV2	DataSync effettua almeno una `LIST` richiesta per ogni oggetto che termina con una barra (`/`) per elencare gli oggetti che iniziano con quel prefisso. Questa richiesta viene chiamata durante la fase di preparazione di un'attività.
HeadObject	DataSync effettua `HEAD` richieste per recuperare i metadati degli oggetti durante le fasi di preparazione e verifica di un'attività. Possono esserci più `HEAD` richieste per oggetto a seconda di come si desidera DataSync verificare l'integrità dei dati trasferiti.
GetObject	DataSync effettua `GET` richieste di lettura dei dati da un oggetto durante la fase di trasferimento di un'attività. Possono esserci più `GET` richieste per oggetti di grandi dimensioni.
GetObjectTagging	Se configuri l'attività per copiare i tag degli oggetti, DataSync effettua queste `GET` richieste per verificare la presenza di tag degli oggetti durante le fasi di preparazione e trasferimento dell'attività.
PutObject	DataSync effettua `PUT` richieste per creare oggetti e prefissi in un bucket S3 di destinazione durante la fase di trasferimento di un'attivi

Richiesta S3	Come DataSync lo usa
	tà. Poiché DataSync utilizza la funzionalità di caricamento multiparte di Amazon S3, possono esserci più PUT richieste per oggetti di grandi dimensioni. Per ridurre al minimo i costi di storage, consigliamo di utilizzare una configura zione del ciclo di vita per impedire caricamenti incompleti in più parti.
PutObjectTagging	Se gli oggetti di origine dispongono di tag e si configura l'attività per copiare i tag degli oggetti, DataSync effettua queste PUT richieste durante il trasferimento di tali tag.
CopyObject	DataSync fa una COPY richiesta per creare una copia di un oggetto solo se i metadati di quell'oggetto cambiano. Ciò può accadere se originariamente hai copiato i dati nel bucket S3 utilizzando un altro servizio o strumento che non trasferiva i relativi metadati.

Considerazioni sui costi

DataSync effettua richieste S3 sui bucket S3 ogni volta che esegui un'attività. Ciò può comportare l'addebito di addebiti in determinate situazioni. Per esempio:

- Trasferisci spesso oggetti da o verso un bucket S3.
- Forse non stai trasferendo molti dati, ma il tuo bucket S3 contiene molti oggetti. In questo scenario è comunque possibile riscontrare costi elevati perché DataSync effettua richieste S3 su ciascuno degli oggetti del bucket.
- Stai effettuando il trasferimento tra i bucket S3, così DataSync come le richieste S3 sull'origine e sulla destinazione.

Per ridurre al minimo i costi delle richieste S3 relative a DataSync, considera quanto segue:

Argomenti

- Quali classi di storage S3 sto utilizzando?
- Con che frequenza devo trasferire i miei dati?

Quali classi di storage S3 sto utilizzando?

I costi delle richieste S3 possono variare in base alla classe di storage Amazon S3 utilizzata dagli oggetti, in particolare per le classi che archiviano oggetti (come S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive).

Ecco alcuni scenari in cui le classi di storage possono influire sui costi delle richieste S3 quando si utilizza: DataSync

- Ogni volta che esegui un'attività, DataSync effettua `HEAD` richieste per recuperare i metadati degli oggetti. Queste richieste comportano addebiti anche se non sposti alcun oggetto. L'impatto di queste richieste sulla fattura dipende dalla classe di archiviazione utilizzata dagli oggetti e dal numero di oggetti sottoposti a DataSync scansione.
- Se hai spostato oggetti nella classe di storage S3 Glacier Instant Retrieval (direttamente o tramite una configurazione del ciclo di vita del bucket), le richieste sugli oggetti di questa classe sono più costose rispetto agli oggetti in altre classi di storage.
- Se configuri l' DataSync attività per verificare che le posizioni di origine e destinazione siano completamente sincronizzate, ci saranno `GET` richieste per ogni oggetto in tutte le classi di archiviazione (tranne S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive).
- Oltre alle `GET` richieste, sono previsti costi di recupero dei dati per gli oggetti nella classe di storage S3 Standard-IA, S3 One Zone-IA o S3 Glacier Instant Retrieval.

Per ulteriori informazioni, consulta Prezzi di Amazon S3.

Con che frequenza devo trasferire i miei dati?

Se devi spostare i dati su base ricorrente, pensa a una pianificazione che non preveda più attività del necessario.

Potresti anche prendere in considerazione la possibilità di limitare la portata dei tuoi trasferimenti. Ad esempio, puoi configurare di DataSync concentrarti sugli oggetti in determinati prefissi o filtrare i dati che vengono trasferiti. Queste opzioni possono aiutare a ridurre il numero di richieste S3 effettuate ogni volta che esegui un'attività. DataSync

Considerazioni sugli oggetti con i trasferimenti Amazon S3

- Se esegui il trasferimento da un bucket S3, usa S3 Storage Lens per determinare quanti oggetti stai spostando.
- Quando effettui il trasferimento tra bucket S3, ti consigliamo di utilizzare la modalità attività avanzata perché non sei soggetto a quote di attività. DataSync
- DataSync potrebbe non trasferire un oggetto con caratteri non standard nel nome. Per ulteriori informazioni, consulta le linee guida per la denominazione delle chiavi degli oggetti nella Amazon S3 User Guide.
- Quando lo utilizzi DataSync con un bucket S3 che utilizza il controllo delle versioni, ricorda quanto segue:
  - Quando si trasferisce in un bucket S3, DataSync crea una nuova versione di un oggetto se tale oggetto viene modificato all'origine. Ciò comporta costi aggiuntivi.
  - Un oggetto ha una versione diversa IDs nei bucket di origine e di destinazione.
- Dopo aver inizialmente trasferito i dati da un bucket S3 a un file system (ad esempio, NFS o FSx Amazon), le esecuzioni successive della DataSync stessa attività non includeranno oggetti che sono stati modificati ma che hanno le stesse dimensioni del primo trasferimento.

Creazione della località di trasferimento per un bucket Amazon S3 generico

Per creare una posizione per il trasferimento, è necessario un bucket S3 per uso generico esistente. Se non ne hai uno, consulta la Amazon S3 User Guide.

> **Important**
>
> Prima di creare la tua posizione, assicurati di leggere le seguenti sezioni:
>
> - Considerazioni sulla classe di storage con Amazon S3 Transfers
> - Valutazione dei costi delle richieste S3 durante l'utilizzo DataSync

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.

3. Per il tipo di posizione, scegli Amazon S3, quindi scegli Bucket per uso generico.
4. Per l'URI S3, inserisci o scegli il bucket e il prefisso che desideri utilizzare per la tua posizione.

   > **Warning**
   >
   > DataSync non è possibile trasferire oggetti con un prefisso che inizia con una barra (/) o include//, o pattern. `/./` `/../` Per esempio:
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`

5. Per la classe di storage S3 utilizzata come destinazione, scegli una classe di storage che desideri che i tuoi oggetti utilizzino quando Amazon S3 è una destinazione di trasferimento.

   Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con Amazon S3 Transfers.
6. In IAM role (Ruolo IAM), eseguire una delle seguenti operazioni:

   - Scegli Autogenerate for per DataSync creare automaticamente un ruolo IAM con le autorizzazioni necessarie per accedere al bucket S3.

     Se DataSync in precedenza hai creato un ruolo IAM per questo bucket S3, quel ruolo viene scelto per impostazione predefinita.
   - Scegli un ruolo IAM personalizzato che hai creato. Per ulteriori informazioni, consulta Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3.
7. (Facoltativo) Scegli Aggiungi nuovo tag per etichettare la tua posizione Amazon S3.

   I tag ti aiutano a gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.
8. Scegli Crea posizione.

Usando il AWS CLI

1. Copia il seguente `create-location-s3` comando:

```
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. Per `--s3-bucket-arn`, specifica l'ARN del bucket S3 che desideri utilizzare come posizione.
3. Per `--s3-storage-class`, specifica una classe di storage che desideri che i tuoi oggetti utilizzino quando Amazon S3 è una destinazione di trasferimento.
4. Per `--s3-config`, specifica l'ARN del ruolo IAM che DataSync deve accedere al tuo bucket.

   Per ulteriori informazioni, consulta Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3.
5. Per `--subdirectory`, specifica un prefisso nel bucket S3 da cui DataSync leggere o scrivere (a seconda che il bucket sia una posizione di origine o di destinazione).

   > **Warning**
   >
   > DataSync non può trasferire oggetti con un prefisso che inizia con una barra (`/`) o include o pattern. `//` `/./` `/../` Per esempio:
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`
6. Esegui il comando `create-location-s3`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN della posizione creata. Per esempio:

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

È possibile utilizzare questa posizione come origine o destinazione per l' DataSync attività.

Creazione della località di trasferimento per un bucket S3 on Outposts

Per creare una sede per il trasferimento, è necessario un bucket Amazon S3 on Outposts esistente. Se non ne hai uno, consulta la Guida per l'utente di Amazon S3 on Outposts.

È inoltre necessario un DataSync agente. Per ulteriori informazioni, consulta Implementazione del tuo agente su AWS Outposts.

Quando esegui il trasferimento da un prefisso del bucket S3 on Outposts che contiene un set di dati di grandi dimensioni (ad esempio centinaia di migliaia o milioni di oggetti), l'attività potrebbe scadere. DataSync Per evitare ciò, prendi in considerazione l'utilizzo di un DataSync manifesto, che ti consente di specificare gli oggetti esatti che devi trasferire.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per il tipo di posizione, scegli Amazon S3, quindi scegli il bucket Outposts.
4. Per il bucket S3, scegli un access point Amazon S3 in grado di accedere al tuo bucket S3 on Outposts.

   Per ulteriori informazioni, consulta la Amazon S3 User Guide.
5. Per la classe di storage S3 utilizzata come destinazione, scegli una classe di storage che desideri che i tuoi oggetti utilizzino quando Amazon S3 è una destinazione di trasferimento.

   Per ulteriori informazioni, consulta. Considerazioni sulla classe di storage con Amazon S3 Transfers DataSync per impostazione predefinita utilizza la classe di storage S3 Outposts per Amazon S3 on Outposts.
6. Per gli agenti, specifica l'Amazon Resource Name (ARN) dell' DataSync agente sul tuo Outpost.
7. Per Folder, inserisci un prefisso nel bucket S3 da cui eseguire la DataSync lettura o la scrittura (a seconda che il bucket sia una posizione di origine o di destinazione).

   > **Warning**
   >
   > DataSync non può trasferire oggetti con un prefisso che inizia con una barra (`/`) o include o pattern. `//` `/./` `/../` Per esempio:

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

8. In IAM role (Ruolo IAM), eseguire una delle seguenti operazioni:

   - Scegli Autogenerate per DataSync creare automaticamente un ruolo IAM con le autorizzazioni necessarie per accedere al bucket S3.

     Se DataSync in precedenza hai creato un ruolo IAM per questo bucket S3, quel ruolo viene scelto per impostazione predefinita.

   - Scegli un ruolo IAM personalizzato che hai creato. Per ulteriori informazioni, consulta Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3.

9. (Facoltativo) Scegli Aggiungi nuovo tag per etichettare la tua posizione Amazon S3.

   I tag ti aiutano a gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.

10. Scegli Crea posizione.

Usando il AWS CLI

1. Copia il seguente `create-location-s3` comando:

```
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. Per`--s3-bucket-arn`, specifica l'ARN, un punto di accesso Amazon S3 che può accedere al tuo bucket S3 on Outposts.

   Per ulteriori informazioni, consulta la Amazon S3 User Guide.

3. Per`--s3-storage-class`, specifica una classe di storage che desideri che i tuoi oggetti utilizzino quando Amazon S3 è una destinazione di trasferimento.

   Per ulteriori informazioni, consultaConsiderazioni sulla classe di storage con Amazon S3 Transfers. DataSync per impostazione predefinita utilizza la classe di archiviazione S3 Outposts per S3 su Outposts.

4. Per`--s3-config`, specifica l'ARN del ruolo IAM che DataSync deve accedere al tuo bucket.

   Per ulteriori informazioni, consulta Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3.

5. Per`--subdirectory`, specifica un prefisso nel bucket S3 da cui DataSync leggere o scrivere (a seconda che il bucket sia una posizione di origine o di destinazione).

   > **Warning**
   >
   > DataSync non può trasferire oggetti con un prefisso che inizia con una barra (`/`) o include o pattern. `//` `/./` `/../` Per esempio:
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`

6. Per`--agent-arns`, specifica l'ARN dell' DataSync agente sul tuo Outpost.
7. Esegui il comando `create-location-s3`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN della posizione creata. Per esempio:

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

È possibile utilizzare questa posizione come origine o destinazione per l' DataSync attività.

Trasferimenti su Amazon S3 Account AWS

Con DataSync, puoi spostare i dati da o verso i bucket S3 in diversi modi. Account AWS Per ulteriori informazioni, consulta i seguenti tutorial:

- Trasferimento di dati dallo storage locale ad Amazon S3 attraverso Account AWS
- Trasferimento di dati da Amazon S3 ad Amazon S3 attraverso Account AWS

Trasferimenti Amazon S3 tra società commerciali e AWS GovCloud (US) Regions

Per impostazione predefinita, DataSync non effettua trasferimenti tra bucket S3 in modalità commerciale e. AWS GovCloud (US) Regions Puoi comunque configurare questo tipo di trasferimento, tuttavia, creando una posizione di archiviazione degli oggetti per uno dei bucket S3 del trasferimento. È possibile eseguire questo tipo di trasferimento con o senza un agente. Se si utilizza un agente, l'operazione deve essere configurata per la modalità Base. Per effettuare il trasferimento senza un agente, è necessario utilizzare la modalità Avanzata.

Prima di iniziare: assicurati di comprendere le implicazioni in termini di costi del trasferimento tra regioni. Per ulteriori informazioni, consulta Prezzi di AWS DataSync.

Indice

- Fornire DataSync l'accesso al bucket della posizione di archiviazione degli oggetti
- Creazione del tuo DataSync agente (opzionale)
- Creazione di una posizione di archiviazione degli oggetti per il tuo bucket S3

Fornire DataSync l'accesso al bucket della posizione di archiviazione degli oggetti

Quando crei la posizione di archiviazione degli oggetti per questo trasferimento, devi fornire DataSync le credenziali di un utente IAM con l'autorizzazione ad accedere al bucket S3 della posizione. Per ulteriori informazioni, consulta Autorizzazioni richieste.

> **Warning**
>
> Gli utenti IAM dispongono di credenziali a lungo termine, il che rappresenta un rischio per la sicurezza. Per ridurre questo rischio, si consiglia di fornire a questi utenti solo le autorizzazioni necessarie per eseguire l'attività e di rimuoverli quando non sono più necessari.

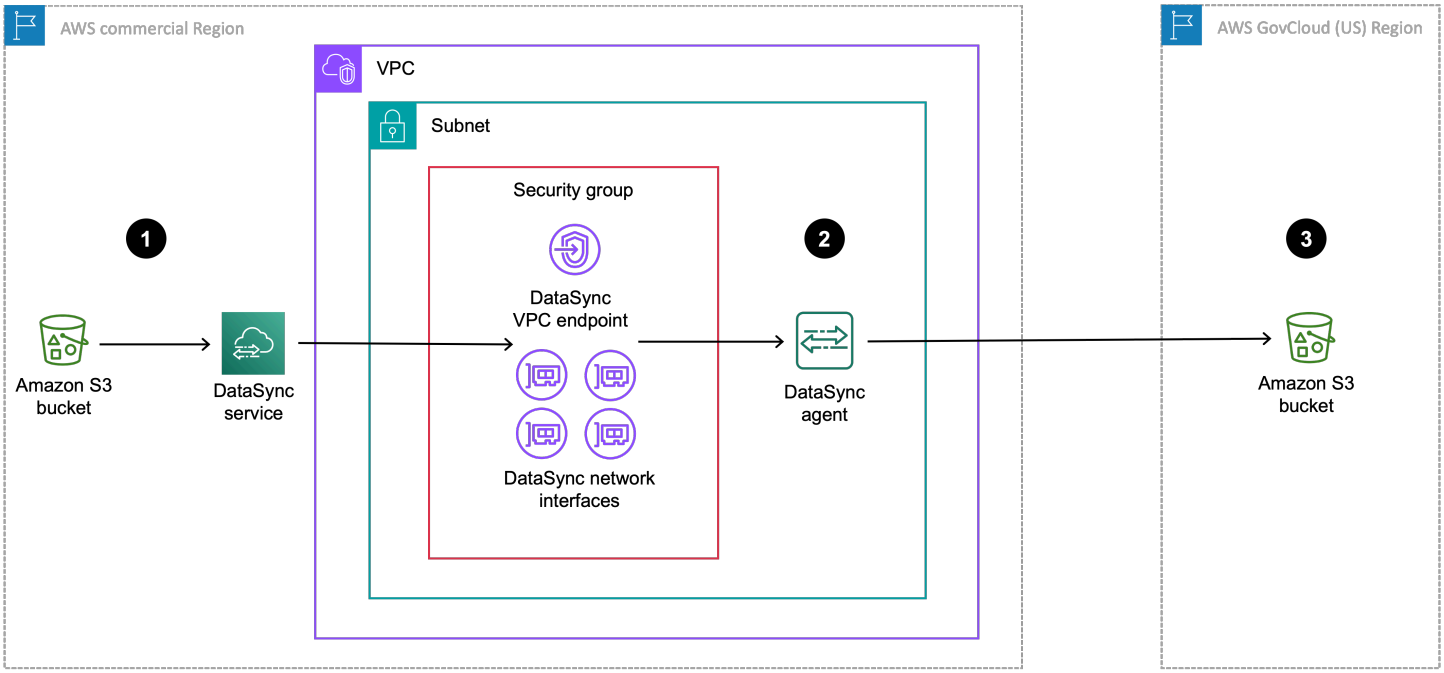
Creazione del tuo DataSync agente (opzionale)

Se desideri eseguire il trasferimento utilizzando la modalità Basic, dovrai utilizzare un agente. Poiché stai effettuando il trasferimento tra una società commerciale e un'altra AWS GovCloud (US) Region, distribuisci il tuo DataSync agente come EC2 istanza Amazon in una delle regioni. Consigliamo al tuo agente di utilizzare un endpoint del servizio VPC per evitare costi di trasferimento dei dati verso la rete Internet pubblica. Per ulteriori informazioni, consulta i prezzi di Amazon EC2 Data Transfer.

Scegli uno dei seguenti scenari che descrivono come creare un agente in base alla regione in cui intendi eseguire l' DataSync attività.

Quando si esegue un' DataSync attività in una regione commerciale

Il diagramma seguente mostra un trasferimento in cui l' DataSync attività e l'agente si trovano nella regione commerciale.



Documentazione di riferimento	Descrizione
1	Nella regione commerciale in cui stai eseguendo un' DataSynca ttività, i dati vengono trasferiti dal bucket S3 di origine. Il bucket di origine è configurato come posizione Amazon S3 nella regione commerciale.

Documentazione di riferimento	Descrizione
2	Trasferimenti di dati tramite l' DataSync agente, che si trova nello stesso VPC e nella stessa sottorete in cui si trovano l'endpoint del servizio VPC e le interfacce di rete.
3	Trasferimenti di dati al bucket S3 di destinazione in. AWS GovCloud (US) Region Il bucket di destinazione è configura to come posizione di archiviazione degli oggetti nella regione commerciale.

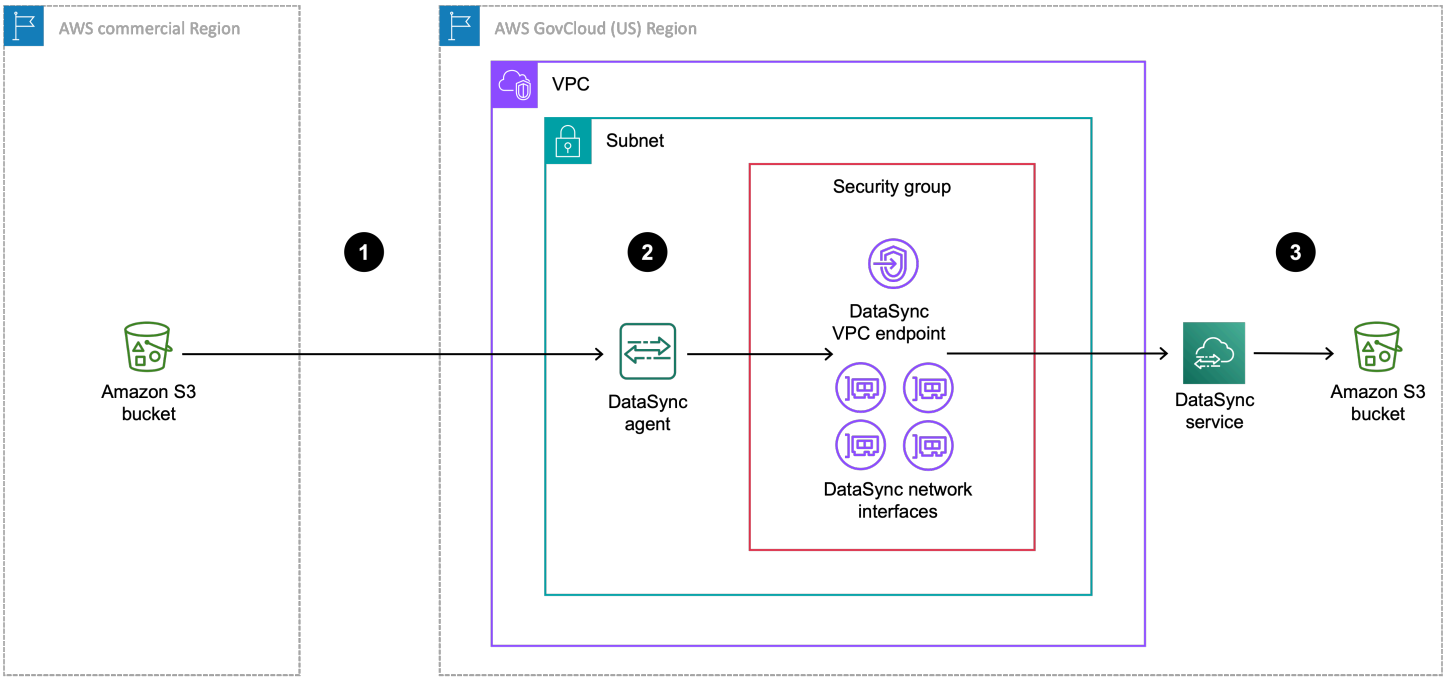
È possibile utilizzare questa stessa configurazione anche per trasferire la direzione opposta dalla AWS GovCloud (US) Region regione commerciale.

Per creare il tuo DataSync agente

1. Implementa un EC2 agente Amazon nella tua regione commerciale.
2. Configura il tuo agente per utilizzare un endpoint del servizio VPC.
3. Attiva il tuo agente.

Quando si esegue un' DataSync attività in una regione GovCloud (Stati Uniti)

Il diagramma seguente mostra un trasferimento in cui si trovano l' DataSync attività e l' AWS GovCloud (US) Region agente in.



Documentazione di riferimento	Descrizione
1	Trasferimenti di dati dal bucket S3 di origine nella regione commerciale al luogo in AWS GovCloud (US) Region cui stai eseguendo un'attività. DataSync Il bucket di origine è configurato come posizione di archiviazione degli oggetti in. AWS GovCloud (US) Region
2	In AWS GovCloud (US) Region, i dati vengono trasferiti tramite l' DataSync agente nello stesso VPC e nella stessa sottorete in cui si trovano l'endpoint del servizio VPC e le interfacce di rete.
3	Trasferimenti di dati al bucket S3 di destinazione in. AWS GovCloud (US) Region Il bucket di destinazione è configurato come posizione Amazon S3 in. AWS GovCloud (US) Region

Puoi utilizzare questa stessa configurazione anche per trasferire la direzione opposta dalla AWS GovCloud (US) Region regione commerciale.

Per creare il tuo DataSync agente

1. Implementa un EC2 agente Amazon nel tuo AWS GovCloud (US) Region.

2. Configura il tuo agente per utilizzare un endpoint del servizio VPC.
3. Attiva il tuo agente.

Se il tuo set di dati è altamente comprimibile, potresti ridurre i costi creando invece il tuo agente in una regione commerciale mentre esegui un'attività in una. AWS GovCloud (US) Region Per la creazione di questo agente sono necessarie più configurazioni del normale, inclusa la preparazione dell'agente per l'uso in una regione commerciale. Per informazioni sulla creazione di un agente per questa configurazione, consulta il AWS DataSync blog Move data in and out of AWS GovCloud (US) with.

Creazione di una posizione di archiviazione degli oggetti per il tuo bucket S3

Hai bisogno di una posizione di archiviazione degli oggetti per il bucket S3 che si trovi nella regione in cui non stai eseguendo l'attività. DataSync

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo. https://console.aws.amazon.com/datasync/
2. Assicurati di trovarti nella stessa regione in cui intendi eseguire l'attività.
3. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Sedi e Crea posizione.
4. Per Tipo di posizione, scegli Archiviazione oggetti.
5. Per Agenti, scegli l' DataSync agente che hai creato per questo trasferimento.
6. Per Server, inserisci un endpoint Amazon S3 per il tuo bucket utilizzando uno dei seguenti formati:

   - Bucket per regione commerciale: `s3.your-region.amazonaws.com`
   - AWS GovCloud (US) Region secchio: `s3.your-gov-region.amazonaws.com`

   Per un elenco degli endpoint Amazon S3, consulta la. Riferimenti generali di AWS
7. Per il nome del bucket, inserisci il nome del bucket S3.
8. Per Folder, inserisci un prefisso nel bucket S3 da cui eseguire la DataSync lettura o la scrittura (a seconda che il bucket sia una posizione di origine o di destinazione).

> **Warning**
>
> DataSync non può trasferire oggetti con un prefisso che inizia con una barra (/) o include o pattern. `//` `/./` `/../` Per esempio:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`
> - `photos/../2006/March`

9. Seleziona Richiede credenziali ed esegui le seguenti operazioni:
   - Per la chiave di accesso, inserisci la chiave di accesso per un utente IAM che può accedere al bucket.
   - Per Chiave segreta, inserisci la chiave segreta dello stesso utente IAM.
10. (Facoltativo) Scegli Aggiungi tag per taggare la tua posizione.

    I tag ti aiutano a gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.
11. Scegli Crea posizione.

Utilizzo di AWS CLI

1. Copia il seguente `create-location-object-storage` comando:

```
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. Per il `--server-hostname` parametro, specifica un endpoint Amazon S3 per il tuo bucket utilizzando uno dei seguenti formati:
   - Bucket per regione commerciale: `s3.your-region.amazonaws.com`
   - AWS GovCloud (US) Region secchio: `s3.your-gov-region.amazonaws.com`

Per la regione nell'endpoint, assicurati di specificare la stessa regione in cui intendi eseguire l'attività.

Per un elenco degli endpoint Amazon S3, consulta la. Riferimenti generali di AWS

3. Per il `--bucket-name` parametro, specifica il nome del bucket S3.
4. Per il `--agent-arns` parametro, specifica l' DataSyncagente che hai creato per questo trasferimento.
5. Per il `--access-key` parametro, specifica la chiave di accesso per un utente IAM che può accedere al bucket.
6. Per il `--secret-key` parametro, inserisci la chiave segreta dello stesso utente IAM.
7. (Facoltativo) Per il `--subdirectory` parametro, specifica un prefisso nel bucket S3 da cui eseguire la DataSync lettura o la scrittura (a seconda che il bucket sia una posizione di origine o di destinazione).

   > **Warning**
   >
   > DataSync non è possibile trasferire oggetti con un prefisso che inizia con una barra (/) o include o pattern. `//` `/./` `/../` Per esempio:
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`

8. (Facoltativo) Per il `--tags` parametro, specificate le coppie chiave-valore che rappresentano i tag per la risorsa di localizzazione.

   I tag ti aiutano a gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.
9. Esegui il comando `create-location-object-storage`.

   Riceverai una risposta che ti mostra l'ARN della posizione che hai appena creato.

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

```
}
```

È possibile utilizzare questa posizione come origine o destinazione per l' DataSync attività. Per l'altro bucket S3 in questo trasferimento, crea una posizione Amazon S3.

Passaggi successivi

Alcuni possibili passaggi successivi includono:

1. Se necessario, crea l'altra località. Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
2. Configura le impostazioni delle DataSync attività, ad esempio quali file trasferire, come gestire i metadati, tra le altre opzioni.
3. Imposta una pianificazione per la tua DataSync attività.
4. Configura il monitoraggio per la tua DataSync attività.
5. Inizia la tua attività.

Configurazione dei AWS DataSync trasferimenti con Amazon EFS

Per trasferire dati da o verso il tuo file system Amazon EFS, devi creare una posizione di AWS DataSync trasferimento. DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Fornire DataSync l'accesso ai file system Amazon EFS

La creazione di una posizione implica la comprensione di come DataSync accedere allo storage. Per Amazon EFS, DataSync monta il file system come utente root dal tuo cloud privato virtuale (VPC) utilizzando interfacce di rete.

Indice

- Determinazione della sottorete e dei gruppi di sicurezza per il target di montaggio
- Accesso ai file system con restrizioni
  - Creazione di un ruolo DataSync IAM per l'accesso al file system
  - Esempio di politica del file system che consente DataSync l'accesso

Determinazione della sottorete e dei gruppi di sicurezza per il target di montaggio

Quando crei la tua posizione, specifichi la sottorete e i gruppi di sicurezza che consentono la connessione DataSync a uno degli obiettivi di montaggio del tuo file system Amazon EFS.

La sottorete specificata deve essere localizzata:

- Nello stesso VPC del file system.
- Nella stessa zona di disponibilità di almeno una destinazione di montaggio per il file system.

> **Note**
>
> Non è necessario specificare una sottorete che presenti una destinazione di montaggio del file system.

I gruppi di sicurezza specificati devono consentire il traffico in entrata sulla porta NFS (Network File System) 2049. Per informazioni sulla creazione e l'aggiornamento dei gruppi di sicurezza per i tuoi target di montaggio, consulta la Amazon EFS User Guide.

Specificazione dei gruppi di sicurezza associati a un target di montaggio

È possibile specificare un gruppo di sicurezza associato a una delle destinazioni di montaggio del file system. Consigliamo questo approccio dal punto di vista della gestione della rete.

Specificare gruppi di sicurezza che non sono associati a un target di montaggio

È inoltre possibile specificare un gruppo di sicurezza che non sia associato a una delle destinazioni di montaggio del file system. Tuttavia, questo gruppo di sicurezza deve essere in grado di comunicare con il gruppo di sicurezza di un target di montaggio.

Ad esempio, ecco come è possibile creare una relazione tra il gruppo di sicurezza D (per DataSync) e il gruppo di sicurezza M (per il target di montaggio):

- Il gruppo di sicurezza D, specificato durante la creazione della posizione, deve avere una regola che consenta le connessioni in uscita sulla porta NFS 2049 al gruppo di sicurezza M.
- Il gruppo di sicurezza M, associato al mount target, deve consentire l'accesso in entrata sulla porta NFS 2049 dal gruppo di sicurezza D.

Per trovare il gruppo di sicurezza di un target di montaggio

Le seguenti istruzioni possono aiutarti a identificare il gruppo di sicurezza di un target di montaggio del file system Amazon EFS che desideri utilizzare DataSync per il trasferimento.

1. In AWS CLI, esegui il `describe-mount-targets` comando seguente.

```
aws efs describe-mount-targets \
    --region file-system-region  \
    --file-system-id file-system-id
```

   Questo comando restituisce informazioni sulle destinazioni di montaggio del file system (in modo simile all'output di esempio seguente).

```
{
    "MountTargets": [
        {
            "OwnerId": "111222333444",
            "MountTargetId": "fsmt-22334a10",
            "FileSystemId": "fs-123456ab",
            "SubnetId": "subnet-f12a0e34",
            "LifeCycleState": "available",
            "IpAddress": "11.222.0.123",
            "NetworkInterfaceId": "eni-1234a044"
        }
    ]
}
```

2. Prendi nota del `MountTargetId` valore che desideri utilizzare.
3. Esegui il `describe-mount-target-security-groups` comando seguente usando `MountTargetId` per vedere il gruppo di sicurezza del tuo target di montaggio.

```
aws efs describe-mount-target-security-groups \
    --region file-system-region \
    --mount-target-id mount-target-id
```

Specificate questo gruppo di sicurezza durante la creazione della vostra posizione.

Accesso ai file system con restrizioni

DataSync può trasferire da o verso file system Amazon EFS che limitano l'accesso tramite punti di accesso e policy IAM.

> **Note**
>
> Se DataSync accede a un file system di destinazione tramite un punto di accesso che impone l'identità dell'utente, l'utente e il gruppo POSIX IDs per i dati di origine non vengono conservati se si configura l' DataSync attività per la proprietà della copia. I file e le cartelle trasferiti vengono invece impostati sull'utente e sul gruppo del punto di accesso. IDs In questo caso, la verifica delle attività non riesce perché DataSync rileva una mancata corrispondenza tra i metadati nelle posizioni di origine e di destinazione.

Indice

- Creazione di un ruolo DataSync IAM per l'accesso al file system
- Esempio di politica del file system che consente DataSync l'accesso

Creazione di un ruolo DataSync IAM per l'accesso al file system

Se disponi di un file system Amazon EFS che limita l'accesso tramite una policy IAM, puoi creare un ruolo IAM che fornisca DataSync l'autorizzazione a leggere o scrivere dati sul file system. Potrebbe quindi essere necessario specificare quel ruolo nella politica del file system.

Per creare il ruolo DataSync IAM

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli, quindi scegli Crea ruolo.
3. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli Politica di attendibilità personalizzata.
4. Incolla il seguente codice JSON nell'editor delle politiche:

   JSON

```
{
```

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

5. Scegli Next (Successivo). Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
6. Dai un nome al tuo ruolo e scegli Crea ruolo.

Specifichi questo ruolo quando crei la tua sede.

Esempio di politica del file system che consente DataSync l'accesso

Il seguente esempio di politica del file system mostra come l'accesso a un file system Amazon EFS (identificato nella policy come`fs-`*`1234567890abcdef0`*) sia limitato ma consenta comunque l'accesso DataSync tramite un ruolo IAM denominato*`MyDataSyncRole`*:

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`— Speciifica un ruolo IAM che DataSync autorizza l'accesso al file system.
- `Action`— Fornisce l'accesso DataSync root e gli consente di leggere e scrivere sul file system.
- `aws:SecureTransport`— Richiede ai client NFS di utilizzare TLS durante la connessione al file system.
- `elasticfilesystem:AccessPointArn`— Consente l'accesso al file system solo tramite un punto di accesso specifico.

Considerazioni sulla rete con i trasferimenti Amazon EFS

VPCs che utilizzi con DataSync deve avere una locazione predefinita. VPCs con locazione dedicata non sono supportati.

Considerazioni sulle prestazioni con i trasferimenti Amazon EFS

La modalità di throughput del file system Amazon EFS può influire sulla durata del trasferimento e sulle prestazioni del file system durante il trasferimento. Considera i seguenti aspetti:

- Per ottenere i migliori risultati, consigliamo di utilizzare la modalità Elastic Throughput. Se non utilizzi la modalità Elastic Throughput, il trasferimento potrebbe richiedere più tempo.
- Se si utilizza la modalità Bursting throughput, le prestazioni delle applicazioni del file system potrebbero risentirne, in quanto DataSync consuma crediti burst del file system.
- La configurazione DataSync per verificare i dati trasferiti può influire sulle prestazioni del file system e sui costi di accesso ai dati.

Per ulteriori informazioni, consulta le prestazioni di Amazon EFS nella Amazon Elastic File System User Guide e nella pagina dei prezzi di Amazon EFS.

Creazione della tua posizione di trasferimento Amazon EFS

Per creare la posizione di trasferimento, è necessario un file system Amazon EFS esistente. Se non ne hai uno, consulta la sezione Guida introduttiva ad Amazon EFS nella Amazon Elastic File System User Guide.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per il tipo di posizione, scegli il file system Amazon EFS.

   Sarà possibile configurare questa posizione come origine o destinazione in un secondo momento.
4. Per File system, scegli il file system Amazon EFS che desideri utilizzare come posizione.
5. Per Mount path, inserisci un percorso di montaggio per il tuo file system Amazon EFS.

   Questo specifica dove DataSync legge o scrive i dati (a seconda che si tratti di una posizione di origine o di destinazione) sul file system.

   Per impostazione predefinita, DataSync utilizza la directory principale (o il punto di accesso, se ne fornisci uno per l'impostazione del punto di accesso EFS). È inoltre possibile specificare le sottodirectory utilizzando barre (ad esempio,). `/path/to/directory`
6. Per Subnet, scegliete una sottorete in cui desiderate creare le interfacce di rete DataSync per la gestione del traffico di trasferimento dati.

   La sottorete deve trovarsi:

   - Nello stesso VPC del file system.
   - Nella stessa zona di disponibilità di almeno una destinazione di montaggio del file system.

> **Note**
>
> Non è necessario specificare una sottorete che presenti una destinazione di montaggio del file system.

7. Per i gruppi di sicurezza, scegli il gruppo di sicurezza associato alla destinazione di montaggio del tuo file system Amazon EFS. Puoi scegliere più di un gruppo di sicurezza.

   > **Note**
   >
   > I gruppi di sicurezza specificati devono consentire il traffico in entrata sulla porta NFS 2049. Per ulteriori informazioni, consulta Determinazione della sottorete e dei gruppi di sicurezza per il target di montaggio.

8. Per la crittografia in transito, scegliete se DataSync utilizzare la crittografia Transport Layer Security (TLS) quando trasferisce i dati da o verso il file system.

   > **Note**
   >
   > Devi abilitare questa impostazione per configurare un punto di accesso, un ruolo IAM o entrambi con la tua posizione Amazon EFS.

9. (Facoltativo) Per il punto di accesso EFS, scegliete un punto di accesso da DataSync utilizzare per montare il file system.

   Per ulteriori informazioni, consulta Accesso ai file system con restrizioni.

10. (Facoltativo) Per il ruolo IAM, specificate un ruolo che DataSync consenta di accedere al file system.

    Per informazioni su come creare questo ruolo, consultare Creazione di un ruolo DataSync IAM per l'accesso al file system.

11. (Facoltativo) Seleziona Aggiungi tag per etichettare il tuo file system.

    Un tag è una coppia chiave-valore che aiuta a gestire, filtrare e cercare le posizioni.

12. Scegli Crea posizione.

Usando il AWS CLI

1. Copia il seguente `create-location-efs` comando:

```
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. Per`--efs-filesystem-arn`, specifica l'Amazon Resource Name (ARN) del file system Amazon EFS da cui stai effettuando il trasferimento.
3. Per`--subdirectory`, specifica un percorso di montaggio per il tuo file system.

   È qui che DataSync legge o scrive i dati (a seconda che si tratti di una posizione di origine o di destinazione) sul file system.

   Per impostazione predefinita, DataSync utilizza la directory principale (o il punto di accesso, se fornito`--access-point-arn`). È inoltre possibile specificare le sottodirectory utilizzando barre (ad esempio,). `/path/to/directory`
4. Per `--ec2-config`, eseguire le seguenti operazioni:

   - Per`SecurityGroupArns`, specifica l'ARN del gruppo di sicurezza associato alla destinazione di montaggio del file system. È possibile specificare più di un gruppo di sicurezza.

     > **Note**
     >
     > I gruppi di sicurezza specificati devono consentire il traffico in entrata sulla porta NFS 2049. Per ulteriori informazioni, consulta Determinazione della sottorete e dei gruppi di sicurezza per il target di montaggio.

   - Per`SubnetArn`, specifica l'ARN della sottorete in cui desideri creare le interfacce DataSync di rete per la gestione del traffico di trasferimento dati.

La sottorete deve trovarsi:

- Nello stesso VPC del file system.
- Nella stessa zona di disponibilità di almeno una destinazione di montaggio del file system.

> **Note**
>
> Non è necessario specificare una sottorete che presenti una destinazione di montaggio del file system.

5. Per`--in-transit-encryption`, specifica se desideri DataSync utilizzare la crittografia Transport Layer Security (TLS) quando trasferisce dati da o verso il tuo file system.

> **Note**
>
> Devi impostarlo su `TLS1_2` per configurare un punto di accesso, un ruolo IAM o entrambi con la tua posizione Amazon EFS.

6. (Facoltativo) Per`--access-point-arn`, specificare l'ARN di un punto di accesso che DataSync può essere utilizzato per montare il file system.

   Per ulteriori informazioni, consulta Accesso ai file system con restrizioni.

7. (Facoltativo) Per`--file-system-access-role-arn`, specifica l'ARN di un ruolo IAM che consente di accedere DataSync al file system.

   Per informazioni su come creare questo ruolo, consultare Creazione di un ruolo DataSync IAM per l'accesso al file system.

8. Esegui il comando `create-location-efs`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN della posizione creata. Per esempio:

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

Configurazione dei trasferimenti con FSx per Windows File Server

Per trasferire dati da o verso il tuo file system Amazon FSx for Windows File Server, devi creare una posizione di AWS DataSync trasferimento. DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Fornire DataSync l'accesso FSx ai file system Windows File Server

DataSync si connette al file system FSx per Windows File Server con il protocollo Server Message Block (SMB) e lo monta dal tuo cloud privato virtuale (VPC) utilizzando interfacce di rete.

> **Note**
>
> VPCs quello che usi con DataSync deve avere una locazione predefinita. VPCs con locazione dedicata non sono supportati.

Argomenti

- Autorizzazioni richieste
- Protocolli di autenticazione richiesti
- Namespace DFS

Autorizzazioni richieste

È necessario fornire a DataSync un utente i diritti necessari per montare e accedere ai file, alle cartelle e ai metadati dei file FSx per Windows File Server.

È consigliabile che questo utente appartenga a un gruppo di Microsoft Active Directory per l'amministrazione del file system. Le specifiche di questo gruppo dipendono dalla configurazione di Active Directory in uso:

- Se utilizzi AWS Directory Service for Microsoft Active Directory with FSx for Windows File Server, l'utente deve essere un membro del gruppo AWS Delegated FSx Administrators.
- Se utilizzi Active Directory autogestito con FSx per Windows File Server, l'utente deve essere membro di uno dei due gruppi:
  - Il gruppo Domain Admins, che è il gruppo di amministratori delegati predefinito.

- Un gruppo di amministratori delegati personalizzato con diritti utente che consentono di copiare le autorizzazioni di proprietà degli oggetti e DataSync gli elenchi di controllo degli accessi di Windows (). ACLs

  > **Important**
  >
  > Non è possibile modificare il gruppo di amministratori delegati dopo la distribuzione del file system. È necessario ridistribuire il file system o ripristinarlo da un backup per utilizzare il gruppo di amministratori delegati personalizzato con i seguenti diritti utente che devono copiare i metadati. DataSync

Diritto dell'utente	Descrizione
Ripristinare file e directory () `SE_RESTORE_NAME`	Consente di DataSync copiare la proprietà degli oggetti, le autorizzazioni, i metadati dei file e gli elenchi di accesso discrezionali NTFS (). DACLs Questo diritto utente viene in genere concesso ai membri dei gruppi Domain Admins e Backup Operators (entrambi gruppi Active Directory predefiniti).
Gestisci i registri di controllo e sicurezza () `SE_SECURITY_NAME`	Consente di copiare DataSync gli elenchi di controllo degli accessi al sistema NTFS ()SACLs. Questo diritto utente viene generalmente concesso ai membri del gruppo Domain Admins.

- Se desideri copiare Windows ACLs e stai effettuando un trasferimento tra un file server SMB e FSx un file system Windows File Server o tra FSx file system Windows File Server, gli utenti forniti DataSync devono appartenere allo stesso dominio Active Directory o avere una relazione di trust Active Directory tra i rispettivi domini.

> **Warning**
>
> L'utente SYSTEM del file system FSx for Windows File Server deve disporre delle autorizzazioni di controllo completo su tutte le cartelle del file system. Non modificate le autorizzazioni ACL NTFS per questo utente sulle vostre cartelle. In tal caso, è DataSync possibile modificare le autorizzazioni del file system in modo da rendere inaccessibile la condivisione dei file e impedire l'utilizzo dei backup del file system. Per ulteriori informazioni sull'accesso a livello di file e cartella, consulta la Amazon FSx for Windows File Server User Guide.

Protocolli di autenticazione richiesti

Il file server FSx per Windows deve utilizzare l'autenticazione NTLM DataSync per accedervi. DataSyncnon può accedere a un file server che utilizza l'autenticazione Kerberos.

Namespace DFS

DataSync non supporta i namespace Microsoft Distributed File System (DFS). Ti consigliamo invece di specificare un file server o una condivisione sottostante quando crei la tua posizione. DataSync

Per ulteriori informazioni, consulta Raggruppamento di più file system con namespace DFS nella Guida per l'utente di FSx Amazon for Windows File Server.

Creazione della posizione di trasferimento FSx per Windows File Server

Prima di iniziare, assicurati di avere un File Server esistente FSx per Windows nel tuo Regione AWS. Per ulteriori informazioni, consulta la sezione Guida introduttiva ad Amazon FSx nella Guida FSx per l'utente di Amazon per Windows File Server.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per il tipo di località, scegli Amazon FSx.
4. Per FSx il file system, scegli il FSx file system Windows File Server che desideri utilizzare come posizione.

5. Per Condividi nome, inserite un percorso di montaggio FSx per il vostro Windows File Server utilizzando le barre.

   Questo specifica il percorso in cui vengono DataSync letti o scritti i dati (a seconda che si tratti di una posizione di origine o di destinazione).

   È inoltre possibile includere sottodirectory (ad esempio,). `/path/to/directory`
6. Per i gruppi di sicurezza, scegli fino a cinque gruppi EC2 di sicurezza Amazon che forniscono l'accesso alla sottorete preferita del tuo file system.

   I gruppi di sicurezza che scegli devono essere in grado di comunicare con i gruppi di sicurezza del tuo file system. Per informazioni sulla configurazione dei gruppi di sicurezza per l'accesso al file system, consulta la Amazon FSx for Windows File Server User Guide.

   > **Note**
   >
   > Se scegli un gruppo di sicurezza che non consente connessioni dall'interno, esegui una delle seguenti operazioni:
   >
   > - Configura il gruppo di sicurezza per consentirgli di comunicare al suo interno.
   > - Scegli un gruppo di sicurezza diverso in grado di comunicare con il gruppo di sicurezza del target di montaggio.
7. Per Utente, inserisci il nome di un utente che può accedere al tuo file server FSx per Windows.

   Per ulteriori informazioni, consulta Autorizzazioni richieste.
8. In Password, inserisci la password del nome utente.
9. (Facoltativo) Per Dominio, immettete il nome del dominio Windows a cui appartiene il file system FSx per Windows File Server.

   Se nell'ambiente sono presenti più domini Active Directory, la configurazione di questa impostazione assicura la DataSync connessione al file system corretto.
10. (Facoltativo) Immettete i valori nei campi Chiave e Valore FSx per etichettare Windows File Server.

    I tag consentono di gestire, filtrare e cercare le AWS risorse. È consigliabile creare almeno un tag di nome per la posizione.
11. Scegli Crea posizione.

Usando il AWS CLI

Per creare una posizione FSx per Windows File Server utilizzando AWS CLI

- Usa il seguente comando per creare una FSx posizione Amazon.

```
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
```

  Nel `create-location-fsx-windows` comando, procedi come segue:

  - `fsx-filesystem-arn`— Specificare l'Amazon Resource Name (ARN) del file system verso o da cui si desidera trasferire.
  - `security-group-arns`— Specificate fino a cinque gruppi ARNs di EC2 sicurezza Amazon che forniscono l'accesso alla sottorete preferita del file system.

    I gruppi di sicurezza specificati devono essere in grado di comunicare con i gruppi di sicurezza del tuo file system. Per informazioni sulla configurazione dei gruppi di sicurezza per l'accesso al file system, consulta la Amazon FSx for Windows File Server User Guide.

    > **Note**
    >
    > Se scegli un gruppo di sicurezza che non consente connessioni dall'interno, esegui una delle seguenti operazioni:
    >
    > - Configura il gruppo di sicurezza per consentirgli di comunicare al suo interno.
    > - Scegli un gruppo di sicurezza diverso in grado di comunicare con il gruppo di sicurezza del target di montaggio.

  - La Regione AWS : la regione specificata è quella in cui si trova il FSx file system Amazon di destinazione.

Questo comando restituisce un ARN di posizione simile a quello mostrato di seguito.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07db7abfc326c50fb"
```

```
}
```

Configurazione dei DataSync trasferimenti con FSx for Lustre

Per trasferire dati da o verso il tuo file system Amazon FSx for Lustre, devi creare una posizione di AWS DataSync trasferimento. DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Fornire DataSync l'accesso ai file FSx system di For Lustre

DataSync accede al file system FSx for Lustre utilizzando il client Lustre. DataSyncrichiede l'accesso a tutti i dati del file system FSx for Lustre. Per avere questo livello di accesso, DataSync installa il file system come utente root utilizzando un ID utente (UID) e un ID di gruppo (GID) di. `0`

DataSync monta il file system dal tuo cloud privato virtuale (VPC) utilizzando interfacce di rete. DataSync gestisce completamente la creazione, l'uso e l'eliminazione di queste interfacce di rete per conto dell'utente.

> **Note**
>
> VPCs che utilizzi con DataSync deve avere una locazione predefinita. VPCs con locazione dedicata non sono supportati.

Creazione della tua località FSx di trasferimento per Lustre

Per creare la posizione di trasferimento, è necessario un file system FSx for Lustre esistente. Per ulteriori informazioni, consulta la sezione Guida introduttiva ad Amazon FSx for Lustre nella Guida per l'utente di Amazon FSx for Lustre.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo. https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per il tipo di località, scegli Amazon FSx.

   Sarà possibile configurare questa posizione come origine o destinazione in un secondo momento.

4. Per FSx il file system, scegli il file system FSx for Lustre che desideri utilizzare come posizione.
5. Per Mount path, inserisci il percorso di montaggio per il tuo file system FSx for Lustre.

   Il percorso può includere una sottodirectory. Quando la posizione viene utilizzata come fonte, DataSync legge i dati dal percorso di montaggio. Quando la posizione viene utilizzata come destinazione, DataSync scrive tutti i dati nel percorso di montaggio. Se non viene fornita una sottodirectory, DataSync utilizza la directory root (`/`).
6. Per i gruppi di sicurezza, scegli fino a cinque gruppi di sicurezza che forniscono l'accesso al file system FSx for Lustre.

   I gruppi di sicurezza devono essere in grado di accedere alle porte del file system. Il file system deve consentire anche l'accesso dai gruppi di sicurezza.

   Per ulteriori informazioni sui gruppi di sicurezza, consulta File System Access Control with Amazon VPC nella Guida per l'utente di Amazon FSx for Lustre.
7. (Facoltativo) Inserisci i valori per i campi Chiave e Valore per etichettare il file system FSx for Lustre.

   I tag ti aiutano a gestire, filtrare e cercare AWS le tue risorse. È consigliabile creare almeno un tag di nome per la posizione.
8. Scegli Crea posizione.

Usando il AWS CLI

Per creare una posizione FSx for Lustre utilizzando il AWS CLI

- Utilizzate il seguente comando per creare una posizione FSx for Lustre.

```
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
```

  Nel `create-location-fsx-lustre` comando sono richiesti i seguenti parametri.

  - `fsx-filesystem-arn`— Il nome Amazon Resource Name (ARN) completo del file system da cui desideri leggere o scrivere.
  - `security-group-arns`— L'ARN di un gruppo di EC2 sicurezza Amazon da applicare alle interfacce di rete della sottorete preferita del file system.

Il comando precedente restituisce un ARN di posizione simile al seguente.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07sb7abfc326c50fb"
}
```

Configurazione dei DataSync trasferimenti con Amazon FSx per OpenZFS

Per trasferire dati da o verso il tuo file system Amazon FSx for OpenZFS, devi creare una posizione di AWS DataSync trasferimento. DataSync può utilizzare questa posizione come fonte o destinazione per il trasferimento di dati.

Fornire DataSync l'accesso FSx ai file system OpenZFS

DataSync monta il file system FSx per OpenZFS dal tuo cloud privato virtuale (VPC) utilizzando interfacce di rete. DataSyncgestisce completamente la creazione, l'uso e l'eliminazione di queste interfacce di rete per vostro conto.

> **Note**
>
> VPCs che utilizzi con DataSync deve avere una locazione predefinita. VPCs con locazione dedicata non sono supportati.

Configurazione FSx per l'autorizzazione del file system OpenZFS

DataSync accede al file system FSx di OpenZFS come client NFS, montando il file system come utente root con un ID utente (UID) e un ID di gruppo (GID) di. `0`

DataSync Per copiare tutti i metadati dei file, è necessario configurare le impostazioni di esportazione NFS sui volumi del file system utilizzando. `no_root_squash` Tuttavia, è possibile limitare questo livello di accesso solo a un'attività specifica DataSync .

Per ulteriori informazioni, consulta le proprietà del volume nella Guida per l'utente di Amazon FSx for OpenZFS.

Configurazione delle esportazioni NFS specifiche per (consigliata) DataSync

Puoi configurare un'esportazione NFS specifica per ogni volume a cui accede solo il tuo task. DataSync Eseguite questa operazione per il volume antenato più recente del percorso di montaggio specificato durante la creazione della posizione FSx per OpenZFS.

Per configurare un'esportazione NFS specifica per DataSync

1. Crea la tua DataSyncattività.

   In questo modo vengono create le interfacce di rete dell'attività specificate nelle impostazioni di esportazione NFS.
2. Individua gli indirizzi IP privati delle interfacce di rete dell'attività utilizzando la EC2 console Amazon o AWS CLI.
3. Per il volume del file system FSx per OpenZFS, configura le seguenti impostazioni di esportazione NFS per ciascuna delle interfacce di rete dell'attività:
   - Indirizzo client: inserisci l'indirizzo IP privato dell'interfaccia di rete (ad esempio,). *10.24.34.0*
   - Opzioni NFS: Invio`rw,no_root_squash`.

Configurazione delle esportazioni NFS per tutti i client

È possibile specificare un'esportazione NFS che consenta l'accesso root a tutti i client.

Per configurare un'esportazione NFS per tutti i client

- Per il volume del file system FSx per OpenZFS, configura le seguenti impostazioni di esportazione NFS:
  - Indirizzo del client: Invio. *
  - Opzioni NFS: Invio`rw,no_root_squash`.

Creazione della posizione di FSx trasferimento per OpenZFS

Per creare la posizione, è necessario un file system esistente FSx per OpenZFS. Se non ne hai uno, consulta la sezione Guida introduttiva ad Amazon FSx for OpenZFS nella Guida per l'utente di Amazon FSx for OpenZFS.

Utilizzo della console di DataSync

1. Apri la console all'indirizzo. AWS DataSync https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione a sinistra, scegli Posizioni, quindi scegli Crea posizione.
3. Per il tipo di località, scegli Amazon FSx.

   Sarà possibile configurare questa posizione come origine o destinazione in un secondo momento.
4. Per FSx il file system, scegli il FSx file system OpenZFS che desideri utilizzare come posizione.
5. Per Mount path, inserisci il percorso di montaggio per il tuo file system FSx per OpenZFS.

   Il percorso deve iniziare con `/fsx` e può essere qualsiasi percorso di directory esistente nel file system. Quando la posizione viene utilizzata come fonte, DataSync legge i dati dal percorso di montaggio. Quando la posizione viene utilizzata come destinazione, DataSync scrive tutti i dati nel percorso di montaggio. Se non viene fornita una sottodirectory, DataSync utilizza la directory del volume principale (ad esempio,`/fsx`).
6. Per i gruppi di sicurezza, scegli fino a cinque gruppi di sicurezza che forniscono l'accesso di rete al tuo file system FSx for OpenZFS.

   I gruppi di sicurezza devono fornire l'accesso alle porte di rete utilizzate dal file system FSx for OpenZFS. Il file system deve consentire l'accesso alla rete dai gruppi di sicurezza.

   Per ulteriori informazioni sui gruppi di sicurezza, consulta Controllo dell'accesso al file system con Amazon VPC nella Guida per l'utente di Amazon FSx for OpenZFS.
7. (Facoltativo) Espandi le impostazioni aggiuntive e per la versione NFS scegli la versione NFS che DataSync utilizza per accedere al tuo file system.

   Per impostazione predefinita, DataSync utilizza la versione NFS 4.1.
8. (Facoltativo) Inserite i valori per i campi Chiave e Valore FSx per etichettare il file system OpenZFS.

   I tag ti aiutano a gestire, filtrare e cercare la tua posizione. È consigliabile creare almeno un tag di nome per la posizione.
9. Scegli Crea posizione.

Usando il AWS CLI

Per creare una posizione FSx per OpenZFS utilizzando il AWS CLI

1. Copia il seguente comando: `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. Specificate le seguenti opzioni obbligatorie nel comando:

   - Per`fsx-filesystem-arn`, specifica il nome Amazon Resource Name (ARN) completo del file system di posizione. Ciò include la posizione Regione AWS in cui risiede il file system Account AWS, il tuo e l'ID del file system.
   - Per`security-group-arns`, specifica l'ARN del gruppo di EC2 sicurezza Amazon che fornisce l'accesso alle interfacce di rete della sottorete preferita del file system FSx for OpenZFS. Ciò include il Regione AWS luogo in cui risiede l' EC2 istanza Amazon Account AWS, il tuo e l'ID del gruppo di sicurezza.

     Per ulteriori informazioni sui gruppi di sicurezza, consulta File System Access Control with Amazon VPC nella Guida per l'utente di Amazon FSx for OpenZFS.
   - Per`protocol`, specifica il protocollo da DataSync utilizzare per accedere al tuo file system. (DataSync attualmente supporta solo NFS).

3. Esegui il comando . Riceverai una risposta che mostra la posizione che hai appena creato.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890"
}
```

Configurazione dei trasferimenti con Amazon FSx for NetApp ONTAP

Per trasferire dati da o verso il tuo file system Amazon FSx for NetApp ONTAP, devi creare una posizione di AWS DataSync trasferimento. DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Fornire DataSync l'accesso FSx ai file system ONTAP

Per accedere a un file system FSx for ONTAP, DataSync monta una macchina virtuale di archiviazione (SVM) sul file system utilizzando interfacce di rete nel cloud privato virtuale (VPC). DataSync crea queste interfacce di rete nella sottorete preferita del file system solo quando create un'attività che include la vostra posizione for ONTAP. FSx

> **Note**
>
> VPCs quello che usi con DataSync deve avere una locazione predefinita. VPCs con locazione dedicata non sono supportati.

DataSync può connettersi a un SVM del file system FSx for ONTAP e copiare i dati utilizzando il protocollo Network File System (NFS) o Server Message Block (SMB).

Argomenti

- Utilizzando il protocollo NFS
- Utilizzo del protocollo SMB
- Protocolli non supportati
- Scegliere il protocollo giusto
- Accesso ai volumi SnapLock

Utilizzando il protocollo NFS

Con il protocollo NFS, DataSync utilizza il meccanismo di `AUTH_SYS` sicurezza con un ID utente (UID) e un ID di gruppo (GID) `0` per l'autenticazione con la SVM.

> **Note**
>
> DataSync attualmente supporta solo la versione 3 di NFS per le sedi ONTAP. FSx

Utilizzo del protocollo SMB

Con il protocollo SMB, DataSync utilizza le credenziali fornite dall'utente per l'autenticazione con la SVM.

Versioni SMB supportate

Per impostazione predefinita, sceglie DataSync automaticamente una versione del protocollo SMB in base alla negoziazione con il file server SMB. Puoi anche configurare l'utilizzo DataSync di una versione specifica, ma ti consigliamo di farlo solo se hai problemi a negoziare DataSync automaticamente con il file server SMB. Per motivi di sicurezza, consigliamo di utilizzare la versione 3.0.2 o successiva di SMB.

Consulta la tabella seguente per un elenco delle opzioni disponibili nella DataSync console e nell'API per configurare una versione SMB con la tua FSx posizione for ONTAP:

Opzione Console	Opzione API	Descrizione
Automatica	`AUTOMATIC`	DataSync e il file server SMB negoziano la versione più recente di SMB che supportano reciprocamente tra la 2.1 e la 3.1.1. Questa è l'opzione predefinita e consigliata. Se scegli una versione specifica che il tuo server di file non supporta, potresti ricevere un errore `Operation Not Supported` .
SMB 3.0.2	`SMB3`	Limita la negoziazione del protocollo alla sola versione SMB 3.0.2.
SMB 2.1	`SMB2`	Limita la negoziazione del protocollo solo alla versione SMB 2.1.
SMB 2.0	`SMB2_0`	Limita la negoziazione del protocollo solo alla versione 2.0 di SMB.

Autorizzazioni richieste

È necessario fornire a DataSync un utente locale nella SVM o a un utente di dominio in Microsoft Active Directory i diritti necessari per montare e accedere a file, cartelle e metadati dei file.

Se specifichi un utente in Active Directory, tieni presente quanto segue:

- Se lo utilizzi AWS Directory Service for Microsoft Active Directory, l'utente deve essere un membro del gruppo AWS Delegated FSx Administrators.
- Se utilizzi un Active Directory autogestito, l'utente deve essere membro di uno dei due gruppi:
  - Il gruppo Domain Admins, che è il gruppo di amministratori delegati predefinito.
  - Un gruppo di amministratori delegati personalizzato con diritti utente che consentono di copiare le autorizzazioni di proprietà degli oggetti e DataSync gli elenchi di controllo degli accessi di Windows (). ACLs

> **Important**
>
> Non è possibile modificare il gruppo di amministratori delegati dopo la distribuzione del file system. È necessario ridistribuire il file system o ripristinarlo da un backup per utilizzare il gruppo di amministratori delegati personalizzato con i seguenti diritti utente che devono copiare i metadati. DataSync

Diritto dell'utente	Descrizione
Funziona come parte del sistema operativo (`SE_TCB_NAME`)	Consente di DataSync copiare la proprietà degli oggetti, le autorizzazioni, i metadati dei file e gli elenchi di accesso discrezionali NTFS (). DACLs Questo diritto utente viene in genere concesso ai membri dei gruppi Domain Admins e Backup Operators (entrambi gruppi Active Directory predefiniti).
Gestisci i registri di controllo e sicurezza () `SE_SECURITY_NAME`	Consente di copiare DataSync gli elenchi di controllo degli accessi al sistema NTFS ()SACLs. Questo diritto utente viene generalmente concesso ai membri del gruppo Domain Admins.

- Se desideri copiare Windows ACLs e stai effettuando il trasferimento tra file system FSx per ONTAP utilizzando SMB (o altri tipi di file system che utilizzano SMB), gli utenti forniti DataSync devono appartenere allo stesso dominio Active Directory o avere una relazione di trust di Active Directory tra i rispettivi domini.

Protocolli di autenticazione richiesti

Per accedere DataSync alla condivisione SMB, il file system FSx for ONTAP deve utilizzare l'autenticazione NTLM. DataSync non è possibile accedere ai FSx file system ONTAP che utilizzano l'autenticazione Kerberos.

Namespace DFS

DataSync non supporta i namespace Microsoft Distributed File System (DFS). Ti consigliamo invece di specificare un file server o una condivisione sottostante quando crei la tua posizione. DataSync

Protocolli non supportati

DataSync non è possibile accedere FSx ai file system ONTAP utilizzando il protocollo iSCSI (Internet Small Computer Systems Interface).

Scegliere il protocollo giusto

Per conservare i metadati dei file FSx per le migrazioni ONTAP, configura le posizioni di DataSync origine e di destinazione in modo che utilizzino lo stesso protocollo. Tra i protocolli supportati, SMB conserva i metadati con la massima fedeltà (vedi per i dettagli). Comprendere come DataSync gestisce i metadati di file e oggetti

Durante la migrazione da un server Unix (Linux) o da una condivisione NAS (Network-Attached Storage) che serve agli utenti tramite NFS, procedi come segue:

1. Crea una posizione NFS per il server Unix (Linux) o la condivisione NAS. (Questa sarà la tua posizione di origine).
2. Configura FSx il volume ONTAP su cui trasferisci i dati con lo stile di sicurezza Unix.
3. Crea una posizione per il tuo file system FSx for ONTAP configurato per NFS. (Questa sarà la tua posizione di destinazione.)

Durante la migrazione da un server Windows o da una condivisione NAS che serve gli utenti tramite SMB, procedi come segue:

1. Crea una posizione SMB per il server Windows o la condivisione NAS. (Questa sarà la tua posizione di origine).
2. Configura FSx il volume ONTAP su cui trasferisci i dati con lo stile di sicurezza NTFS.
3. Crea una posizione per il tuo file system FSx for ONTAP configurato per SMB. (Questa sarà la tua posizione di destinazione).

Se il tuo ambiente FSx for ONTAP utilizza più protocolli, ti consigliamo di rivolgerti a uno specialista AWS dello storage. Per conoscere le best practice per l'accesso multiprotocollo, consulta Enabling multiprotocol workload with Amazon FSx for ONTAP. NetApp

Accesso ai volumi SnapLock

Se trasferisci dati su un SnapLock volume su un file system FSx for ONTAP, assicurati che le SnapLock impostazioni Autocommit e Volume append mode siano disabilitate sul volume durante il trasferimento. Puoi riattivare queste impostazioni al termine del trasferimento dei dati.

Creazione della sede di trasferimento FSx per ONTAP

Per creare la posizione, è necessario un file system esistente FSx per ONTAP. Se non ne hai uno, consulta la sezione Guida introduttiva ad Amazon FSx for NetApp ONTAP nella Guida per l'utente di Amazon FSx for NetApp ONTAP.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo. https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per il tipo di località, scegli Amazon FSx.

   Sarà possibile configurare questa posizione come origine o destinazione in un secondo momento.
4. Per FSx il file system, scegli il FSx file system ONTAP che desideri utilizzare come posizione.
5. Per la macchina virtuale di archiviazione, scegli una macchina virtuale di archiviazione (SVM) nel file system in cui desideri copiare i dati o da cui desideri copiare i dati.
6. Per Mount path, specifica un percorso per la condivisione di file in quella SVM in cui copiare i dati.

Puoi specificare un percorso di giunzione (detto anche punto di montaggio), un percorso qtree (per condivisioni di file NFS) o un nome condivisione (per condivisioni di file SMB). Ad esempio, il percorso di montaggio potrebbe essere `/vol1`, `/vol1/tree1`, o `/share1`.

> **Tip**
>
> Non specificate un percorso nel volume root della SVM. Per ulteriori informazioni, consulta Managing FSx for ONTAP Storage Virtual Machines nella Amazon FSx for NetApp ONTAP User Guide.

7. Per i gruppi di sicurezza, scegli fino a cinque gruppi EC2 di sicurezza Amazon che forniscono l'accesso alla sottorete preferita del tuo file system.

   I gruppi di sicurezza devono consentire il traffico in uscita sulle seguenti porte (a seconda del protocollo utilizzato):

   - NFS: porte TCP 111, 635 e 2049
   - SMB: porta TCP 445

   I gruppi di sicurezza del file system devono inoltre consentire il traffico in entrata sulle stesse porte.

8. Per Protocollo, scegliete il protocollo di trasferimento dati da DataSync utilizzare per accedere alla SVM del file system.

   Per ulteriori informazioni, consulta Scegliere il protocollo giusto.

   NFS

   DataSync utilizza la versione 3 di NFS.

   SMB

   Configurate una versione SMB, un utente, una password e un nome di dominio Active Directory (se necessario) per accedere alla SVM.

   - (Facoltativo) Espandi le impostazioni aggiuntive e scegli una versione SMB DataSync da utilizzare per accedere al tuo SVM.

Per impostazione predefinita, sceglie DataSync automaticamente una versione in base alla negoziazione con il file server SMB. Per ulteriori informazioni, consulta Utilizzo del protocollo SMB.

- Per Utente, inserite un nome utente in grado di montare e accedere ai file, alle cartelle e ai metadati che desiderate trasferire nell'SVM.

  Per ulteriori informazioni, consulta Utilizzo del protocollo SMB.

- Per Password, inserite la password dell'utente specificato che può accedere all'SVM.
- (Facoltativo) Per il nome di dominio Active Directory, inserite il nome di dominio completo (FQDN) dell'Active Directory a cui appartiene la SVM.

  Se nel tuo ambiente sono presenti più domini, la configurazione di questa impostazione assicura che DataSync si connetta all'SVM corretto.

9. (Facoltativo) Inserite i valori per i campi Chiave e Valore per etichettarli FSx per il file system ONTAP.

   I tag ti aiutano a gestire, filtrare e cercare AWS le tue risorse. È consigliabile creare almeno un tag di nome per la posizione.

10. Scegli Crea posizione.

Usando il AWS CLI

Per creare una posizione FSx per ONTAP utilizzando il AWS CLI

1. Copia il seguente `create-location-fsx-ontap` comando:

```
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. Specificate le seguenti opzioni obbligatorie nel comando:

   - Per`storage-virtual-machine-arn`, specifica l'Amazon Resource Name (ARN) completo di una macchina virtuale di storage (SVM) nel file system in cui desideri copiare i dati.

Questo ARN include la posizione Regione AWS in cui risiede il file system Account AWS, il file system e SVM. IDs

- Per`security-group-arns`, specifica i gruppi ARNs di EC2 sicurezza Amazon che forniscono l'accesso alle interfacce di rete della sottorete preferita del tuo file system.

  Ciò include il Regione AWS luogo in cui risiede la tua EC2 istanza Amazon Account AWS, il tuo e il tuo gruppo IDs di sicurezza. Puoi specificare fino a cinque gruppi ARNs di sicurezza.

  Per ulteriori informazioni sui gruppi di sicurezza, consulta File System Access Control with Amazon VPC nella Guida per l'utente di Amazon FSx for NetApp ONTAP.

- Per`protocol`, configura il protocollo da DataSync utilizzare per accedere alla SVM del tuo file system.
  - Per NFS, puoi usare la configurazione predefinita:

    ```
    --protocol NFS={}
    ```

  - Per SMB, è necessario specificare un nome utente e una password che possano accedere all'SVM:

    ```
    --protocol SMB={User=smb-user,Password=smb-password}
    ```

3. Esegui il comando .

   Riceverai una risposta che mostra la posizione che hai appena creato.

   ```
   {
       "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
   abcdef01234567890"
   }
   ```

Trasferimento da o verso un altro spazio di archiviazione cloud con AWS DataSync

Con AWS DataSync, puoi trasferire dati tra altri provider di cloud e servizi AWS di archiviazione. Per ulteriori informazioni, vedi Con dove posso trasferire i miei dati DataSync?

Argomenti

- Pianificazione dei trasferimenti da o verso sistemi di archiviazione cloud di terze parti

- Configurazione dei AWS DataSync trasferimenti con Google Cloud Storage
- Configurazione dei trasferimenti con Microsoft Azure Blob Storage
- Configurazione dei AWS DataSync trasferimenti con Microsoft Azure Files Condivisioni SMB
- Configurazione dei trasferimenti con altri archivi di oggetti nel cloud

Pianificazione dei trasferimenti da o verso sistemi di archiviazione cloud di terze parti

Quando pianifichi trasferimenti di dati tra cloud diversi, considera quanto segue:

- Utilizzo di un agente: un agente è necessario solo per accedere allo storage in altri cloud quando si utilizzano le attività in modalità Basic. Le attività in modalità avanzata non richiedono un agente. Se decidi di utilizzare un agente, puoi distribuirlo come EC2istanza Amazon durante il trasferimento dallo storage di oggetti compatibile con S3 di un provider di cloud o come Google Compute Engine o Azure Virtual Machine per i trasferimenti da quei servizi di archiviazione specifici, rispettivamente. Durante il trasferimento da file system di Google e Azure, consigliamo di distribuire l'agente come macchina virtuale Google o Azure in modo che l'agente sia il più vicino possibile al filesystem. Inoltre, DataSync comprime i dati dall'agente a, il che può aiutare a ridurre i costi di uscita. AWS DataSync fornisce un elenco di posizioni cloud convalidate che forniscono la compatibilità delle API Amazon S3 richiesta.
- L'altro endpoint di storage di oggetti del cloud: l'endpoint di archiviazione per un provider cloud di terze parti è in genere specifico della regione o dell'account. L'endpoint regionale viene utilizzato come server nella posizione di archiviazione degli DataSync oggetti, insieme a un nome di bucket specificato.
- Classi di archiviazione degli oggetti di origine: come Amazon S3, alcuni provider di servizi cloud supportano un livello di archiviazione che richiede un ripristino prima di poter accedere agli oggetti archiviati. Ad esempio, gli oggetti nel livello di archiviazione Azure Blob devono essere recuperati per l'accesso standard prima del trasferimento dei dati. È possibile accedere immediatamente agli oggetti nel livello di archiviazione di Google Cloud Storage e non richiedono il ripristino, ma l'accesso diretto al livello di archiviazione comporta dei costi di recupero. Consulta la documentazione della classe di archiviazione su più cloud per determinare i requisiti di accesso e le tariffe di recupero prima di iniziare il trasferimento dei dati. Per ulteriori informazioni sul ripristino di oggetti archiviati in Amazon S3, consulta Restoring an archived object nella Amazon Simple Storage Service User Guide.

- Accesso allo storage di oggetti: il trasferimento di dati tra provider cloud di terze parti richiede l'accesso all'archiviazione di oggetti dell'altro cloud sotto forma di chiavi di autenticazione. Ad esempio, per fornire l'accesso a Google Cloud Storage, configuri una posizione di archiviazione degli DataSync oggetti che si connette all'API XML di Google Cloud Storage e si autentica utilizzando una chiave HMAC (Message Authentication Code) basata su Hash per il tuo account di servizio. Per l'archiviazione Azure Blob, configuri una posizione Azure DataSync Blob dedicata che si autentica tramite token SAS. DataSync utilizza per archiviare in modo sicuro le credenziali AWS Secrets Manager di archiviazione degli oggetti. Per ulteriori informazioni, vedere Protezione delle credenziali della posizione di archiviazione.
- Supporto per i tag degli oggetti:
  - A differenza di Amazon S3, non tutti i provider di servizi cloud supportano i tag degli oggetti. DataSync le attività possono fallire durante il tentativo di leggere i tag dalla posizione di origine se il provider cloud non supporta i tag degli oggetti tramite l'API Amazon S3 o se le credenziali fornite non sono sufficienti per recuperare i tag. DataSyncfornisce un'opzione task per disattivare la lettura e la copia dei tag degli oggetti durante un trasferimento se i tag degli oggetti non sono supportati o se non si desidera mantenerli. Consulta la documentazione del tuo provider di servizi cloud per determinare se i tag degli oggetti sono supportati e verifica le impostazioni dei tag degli oggetti dell'attività di trasferimento prima di iniziare il trasferimento.
  - Puoi utilizzare l'API Amazon S3 per verificare se un provider di servizi cloud restituirà una `get-object-tagging` richiesta. Per ulteriori informazioni, consulta la sezione get-object-tagging nella Documentazione di riferimento della AWS CLI .

    Un provider di servizi cloud che supporta i tag degli oggetti restituirà una risposta simile al seguente esempio:

    ```
    aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint- url=https://
    BUCKET_ENDPOINT --key prefix/file1

    {

        "TagSet": []

    }
    ```

    Un provider di servizi cloud che non supporta `get-object-tagging` restituirà il seguente messaggio:

```
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
```

- Costi associati per le richieste e l'uscita dei dati: il trasferimento di dati dallo storage di oggetti nel cloud comporta costi di richiesta e uscita associati alla lettura dei dati e al trasferimento dei dati. I costi di richiesta variano tra i provider di servizi cloud e tra le classi di archiviazione, ove applicabile. Consulta la documentazione del tuo provider di servizi cloud in merito ai costi specifici per le richieste relative alla classe di archiviazione da cui intendi leggere. Per una panoramica dei costi di richiesta associati ai trasferimenti DataSync di dati, consulta Valutazione dei costi delle richieste S3 durante l'utilizzo DataSync e AWS DataSync i prezzi. Il trasferimento di dati da provider cloud specifici comporta costi di uscita. I costi di trasferimento dei dati variano tra i provider di servizi cloud e dipendono anche dalla regione in cui sono archiviati i dati.
- Frequenze di richiesta di archiviazione degli oggetti: i provider di servizi cloud hanno diverse caratteristiche di prestazioni e velocità di richiesta per le loro piattaforme di storage di oggetti. Controlla le percentuali di richiesta dell'altro provider di servizi cloud e determina dove vengono applicati i limiti di richiesta. Pianifica in anticipo i trasferimenti altamente parallelizzati composti da più agenti, laddove potrebbero essere necessari specifici partizionamenti o aumenti delle prestazioni.

  Amazon S3 ha tassi di richiesta documentati su cui puoi costruire la tua soluzione. Le frequenze di richiesta di Amazon S3 sono per prefisso partizionato e sono scalabili su più prefissi. Per ulteriori informazioni, consulta Modelli di progettazione basati sulle best practice: ottimizzazione delle prestazioni di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Configurazione dei AWS DataSync trasferimenti con Google Cloud Storage

Il seguente tutorial mostra come eseguire la migrazione di oggetti da un bucket Google Cloud Storage (GCS) a un bucket Amazon S3. AWS DataSync

Panoramica

DataSync utilizza l'API XML di Google Cloud Storage per i trasferimenti di dati. Questa API fornisce un'interfaccia compatibile con Amazon S3 per leggere e scrivere dati con bucket GCS.

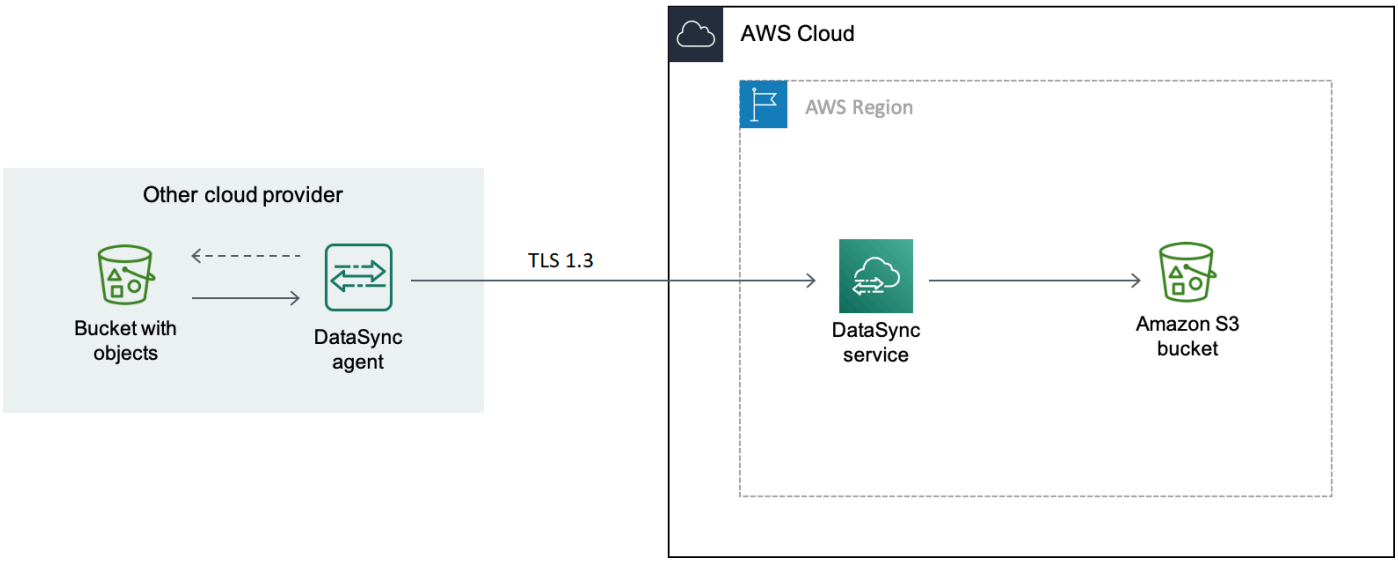
DataSync supporta i trasferimenti tra GCS e i servizi di storage. AWS Quando si esegue la copia tra GCS e Amazon EFS o Amazon FSx, è necessario un agente e l'attività deve utilizzare la modalità Basic. Quando si esegue la copia tra GCS e Amazon S3, è necessario un agente solo quando si utilizza la modalità Basic.

Se utilizzi un agente per il trasferimento, puoi distribuire l'agente in Google Cloud o nel tuo Amazon VPC.

Agent in Google Cloud

1. Implementate un DataSync agente nel vostro ambiente Google Cloud.
2. L'agente legge il tuo bucket Google Cloud Storage utilizzando una chiave HMAC (Message Authentication Code) basata su Hash.
3. Gli oggetti dal tuo bucket Google Cloud Storage vengono trasferiti in modo sicuro tramite TLS 1.3 nel bucket utilizzando un endpoint pubblico. Cloud AWS
4. Il DataSync servizio scrive i dati nel tuo bucket S3.

Il diagramma seguente illustra il trasferimento.

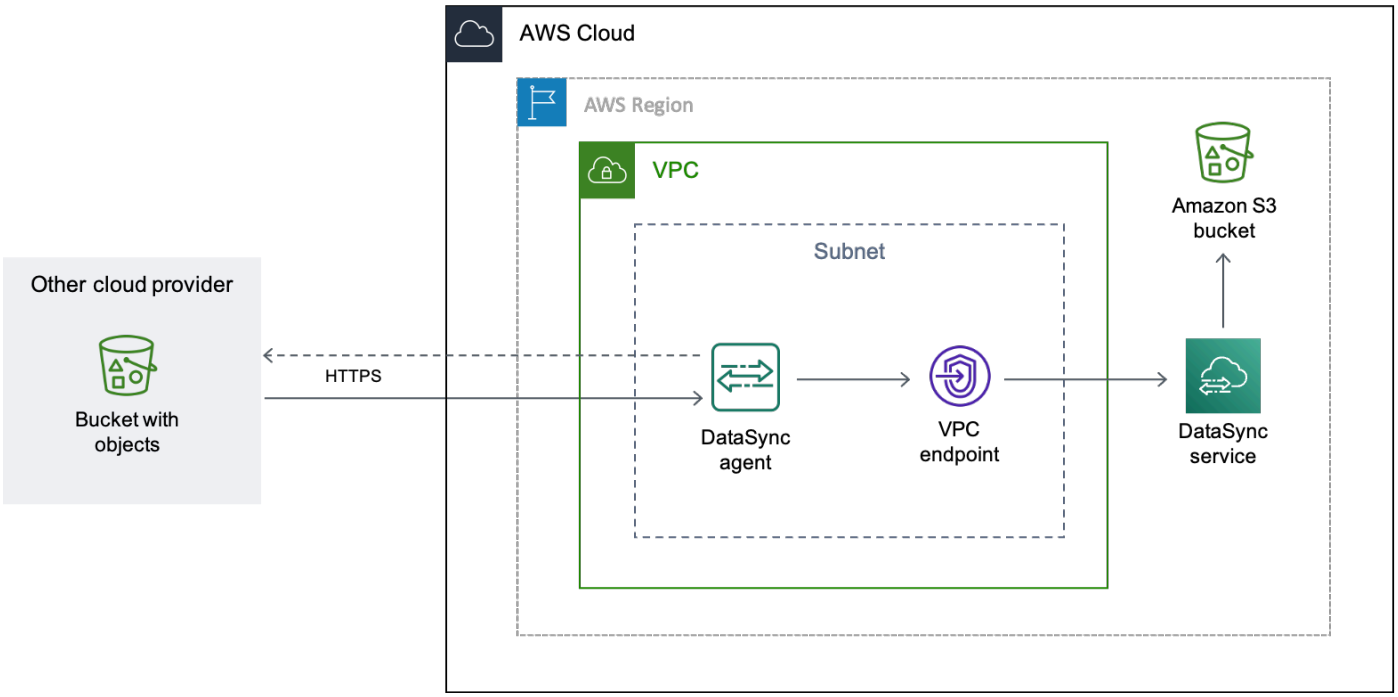


Agent in your VPC

1. Implementate un DataSync agente in un cloud privato virtuale (VPC) nel AWS vostro ambiente.
2. L'agente legge il tuo bucket Google Cloud Storage utilizzando una chiave HMAC (Message Authentication Code) basata su Hash.

3. Gli oggetti dal tuo bucket Google Cloud Storage vengono trasferiti in modo sicuro tramite TLS 1.3 nel bucket Cloud AWS utilizzando un endpoint VPC privato.
4. Il DataSync servizio scrive i dati nel tuo bucket S3.

Il diagramma seguente illustra il trasferimento.



Costi

Le tariffe associate a questa migrazione potrebbero includere:

- Esecuzione di un'istanza di macchina virtuale (VM) di Google Compute Engine (se distribuisci il tuo DataSync agente in Google Cloud)
- Esecuzione di un' EC2istanza Amazon (se distribuisci il tuo DataSync agente in un AWS VPC interno)
- Trasferimento dei dati tramite utilizzo DataSync, inclusi i costi di richiesta relativi a Google Cloud Storage e Amazon S3 (se S3 è una delle tue sedi di trasferimento)
- Trasferimento di dati da Google Cloud Storage
- Archiviazione dei dati in Amazon S3

Prerequisiti

Prima di iniziare, procedi come segue se non l'hai già fatto:

- Crea un bucket Google Cloud Storage con gli oggetti in cui desideri trasferire AWS.
- Iscriviti a un Account AWS.
- Crea un bucket Amazon S3 per archiviare gli oggetti dopo averli inseriti. AWS

Creazione di una chiave HMAC per il tuo bucket Google Cloud Storage

DataSync utilizza una chiave HMAC associata al tuo account di servizio Google per autenticarti e leggere il bucket da cui stai trasferendo i dati. (Per istruzioni dettagliate su come creare chiavi HMAC, consulta la documentazione di Google Cloud Storage.)

Per creare una chiave HMAC

1. Crea una chiave HMAC per il tuo account di servizio Google.
2. Assicurati che il tuo account di servizio Google disponga almeno delle `Storage Object Viewer` autorizzazioni.
3. Salva l'ID di accesso e il segreto della tua chiave HMAC in un luogo sicuro.

   Questi elementi ti serviranno in seguito per configurare la posizione di DataSync origine.

Fase 2: Configurare la rete

La configurazione di rete è richiesta solo quando si utilizza un DataSync agente per il trasferimento. I requisiti di rete per questa migrazione dipendono dal luogo in cui si sceglie di distribuire l'agente.

Per un DataSync agente in Google Cloud

Se desideri ospitare il tuo DataSync agente in Google Cloud, configura la tua rete per consentire DataSync i trasferimenti tramite un endpoint pubblico.

Per un DataSync agente nel tuo VPC

Se desideri ospitare il tuo agente AWS, hai bisogno di un VPC con un endpoint di interfaccia. DataSync utilizza l'endpoint VPC per facilitare il trasferimento.

Per configurare la rete per un endpoint VPC

1. Se non ne hai uno, crea un VPC nello stesso Regione AWS del tuo bucket S3.
2. Crea una sottorete privata per il tuo VPC.
3. Crea un endpoint di servizio VPC per. DataSync
4. Configura la tua rete per consentire DataSync i trasferimenti tramite un endpoint del servizio VPC.

   A tale scopo, modifica il gruppo di sicurezza associato all'endpoint del servizio VPC.

Fase 3: Creare un DataSync agente (opzionale)

Un DataSync agente è necessario solo quando si utilizzano le attività in modalità Basic. Se utilizzi la modalità avanzata per il trasferimento tra Google Cloud Storage (GCS) e Amazon S3, non è richiesto alcun agente. Se desideri utilizzare la modalità Basic, hai bisogno di un DataSync agente in grado di accedere al tuo bucket GCS.

Per Google Cloud

In questo scenario, l' DataSync agente viene eseguito nel tuo ambiente Google Cloud.

Prima di iniziare: installa la CLI di Google Cloud.

Per creare l'agente per Google Cloud

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Agenti, quindi scegli Crea agente.
3. Per Hypervisor, scegli VMware ESXi, quindi scegli Scarica l'immagine per scaricare un `.zip` file che contiene l'agente.
4. Apri un terminale. Decomprimi l'immagine eseguendo il seguente comando:

   ```
   unzip AWS-DataSync-Agent-VMWare.zip
   ```

5. Estrai il contenuto del `.ova` file dell'agente iniziando con `aws-datasync` eseguendo il comando seguente:

   ```
   tar -xvf aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt.ova
   ```

6. Importa il `.vmdk` file dell'agente in Google Cloud eseguendo il seguente comando CLI di Google Cloud:

```
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**
>
> L'importazione del `.vmdk` file potrebbe richiedere fino a due ore.

7. Crea e avvia un'istanza di macchina virtuale per l'immagine dell'agente che hai appena importato.

   L'istanza richiede le seguenti configurazioni per l'agente. (Per istruzioni dettagliate su come creare un'istanza, consulta la documentazione di Google Cloud Compute Engine.)

   - Per il tipo di macchina, scegli una delle seguenti opzioni:
     - e2-standard-8: per l'esecuzione di DataSync attività con un massimo di 20 milioni di oggetti.
     - e2-standard-16 — Per le esecuzioni di DataSync attività che utilizzano più di 20 milioni di oggetti.
   - Per le impostazioni del disco di avvio, vai alla sezione immagini personalizzate. Quindi scegli l'immagine dell' DataSync agente che hai appena importato.
   - Per l'impostazione dell'account di servizio, scegli il tuo account di servizio Google (lo stesso account che hai utilizzato nel passaggio 1).
   - Per l'impostazione del firewall, scegli l'opzione per consentire il traffico HTTP (porta 80).

     Per attivare l' DataSync agente, la porta 80 deve essere aperta sull'agente. Non è necessario che la porta sia accessibile al pubblico. Una volta attivata, DataSync chiude la porta.

8. Dopo l'esecuzione dell'istanza VM, prendi nota del relativo indirizzo IP pubblico.

   Avrai bisogno di questo indirizzo IP per attivare l'agente.

9. Torna alla DataSync console. Nella schermata Crea agente in cui hai scaricato l'immagine dell'agente, procedi come segue per attivare l'agente:

- Per Tipo di endpoint, scegli l'opzione Endpoint di servizio pubblico (ad esempio, Endpoint di servizio pubblico negli Stati Uniti orientali dell'Ohio).
- Per Chiave di attivazione, scegli Ottieni automaticamente la chiave di attivazione dal tuo agente.
- Per l'indirizzo dell'agente, inserisci l'indirizzo IP pubblico dell'istanza di macchina virtuale dell'agente che hai appena creato.
- Scegli Get key.

10. Dai un nome al tuo agente, quindi scegli Crea agente.

Il tuo agente è online e pronto a trasferire i dati.

Per il tuo VPC

In questo scenario, l'agente viene eseguito come EC2 istanza Amazon in un VPC associato al tuo. Account AWS

Prima di iniziare: configura AWS Command Line Interface (AWS CLI).

Per creare l'agente per il tuo VPC

1. Apri un terminale. Assicurati di configurare il tuo AWS CLI profilo per utilizzare l'account associato al tuo bucket S3.
2. Copiare il seguente comando. Sostituisci *vpc-region* con il Regione AWS luogo in cui risiede il tuo VPC (ad esempio,). `us-east-1`

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

3. Esegui il comando . Nell'output, prendi nota della `"Value"` proprietà.

   Questo valore è l'ID DataSync Amazon Machine Image (AMI) della regione specificata. Ad esempio, potrebbe essere simile a un ID AMI`ami-1234567890abcdef0`.

4. Copia il seguente URL. Ancora una volta, *vpc-region* sostituiscilo con il Regione AWS luogo in cui risiede il tuo VPC. Quindi, *ami-id* sostituiscilo con l'ID AMI che hai annotato nel passaggio precedente.

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

5. Incollare l'URL in un browser.

   La pagina di avvio dell' EC2 istanza Amazon AWS Management Console viene visualizzata nei display.
6. Per il tipo di istanza, scegli una delle EC2 istanze Amazon consigliate per DataSync agenti.
7. Per Coppia di chiavi, scegli una coppia di chiavi esistente o creane una nuova.
8. Per le impostazioni di rete, scegli il VPC e la sottorete in cui desideri distribuire l'agente.
9. Scegliere Launch Instance (Avvia istanza).
10. Una volta che l' EC2 istanza Amazon è in esecuzione, scegli il tuo endpoint VPC.
11. Attiva il tuo agente.

Passaggio 4: crea una posizione di DataSync origine per il tuo bucket Google Cloud Storage

Per configurare una DataSync posizione per il tuo bucket Google Cloud Storage, hai bisogno dell'ID di accesso e del segreto per la chiave HMAC che hai creato nel passaggio 1.

Per creare la posizione di origine DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per Tipo di posizione, scegli Archiviazione oggetti.
4. Per Server, immettere**`storage.googleapis.com`**.
5. Per il nome del bucket, inserisci il nome del tuo bucket Google Cloud Storage.
6. Per Folder, inserisci il prefisso di un oggetto.

   DataSync copia solo gli oggetti con questo prefisso.
7. Se il trasferimento richiede un agente, scegli Usa agenti, quindi scegli l'agente che hai creato nel passaggio 3.
8. Espandere Additional settings (Impostazioni aggiuntive). Per il protocollo Server, scegli HTTPS. Per Porta server, scegli 443.
9. Scorri verso il basso fino alla sezione Autenticazione. Assicurati che la casella di controllo Richiede credenziali sia selezionata, quindi procedi come segue:

- Per la chiave di accesso, inserisci l'ID di accesso della tua chiave HMAC.
- Per la chiave segreta, inserisci direttamente la chiave segreta della tua chiave HMAC o specifica un AWS Secrets Manager segreto che contenga la chiave. Per ulteriori informazioni, vedere Fornitura di credenziali per le posizioni di archiviazione.

10. Scegli Crea posizione.

Passaggio 5: crea una posizione di DataSync destinazione per il tuo bucket S3

Ti serve una DataSync posizione in cui desideri che i tuoi dati finiscano.

Per creare la posizione di DataSync destinazione

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Crea una DataSync posizione per il bucket S3.

   Se hai distribuito l' DataSync agente nel tuo VPC, questo tutorial presuppone che il bucket S3 sia nello stesso posto tra VPC e Regione AWS agente. DataSync

Passaggio 6: creare e avviare un'attività DataSync

Una volta configurate le posizioni di origine e di destinazione, puoi iniziare a trasferire i tuoi dati AWS.

Per creare e avviare l' DataSync attività

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Nella pagina Configura la posizione di origine, procedi come segue:

   a. Scegli una posizione esistente.

   b. Scegli la posizione di origine che hai creato nel passaggio 4, quindi scegli Avanti.

4. Nella pagina Configura la posizione di destinazione, procedi come segue:

   a. Scegli una posizione esistente.

b. Scegli la posizione di destinazione che hai creato nel passaggio 5, quindi scegli Avanti.

5. Nella pagina Configura impostazioni, procedi come segue:

   a. In Configurazione del trasferimento dati, espandi Impostazioni aggiuntive e deseleziona la casella di controllo Copia i tag degli oggetti.

   > **Important**
   >
   > Poiché l'API XML di Google Cloud Storage non supporta la lettura o la scrittura di tag di oggetto, l' DataSync operazione potrebbe non riuscire se provi a copiare i tag degli oggetti.

   b. Configura tutte le altre impostazioni dell'attività che desideri, quindi scegli Avanti.

6. Nella pagina Revisione, rivedi le impostazioni, quindi scegli Crea attività.

7. Nella pagina dei dettagli dell'attività, scegli Avvia, quindi scegli una delle seguenti opzioni:

   - Per eseguire l'attività senza modifiche, scegli Inizia con i valori predefiniti.
   - Per modificare l'attività prima di eseguirla, scegli Inizia con opzioni di sovrascrittura.

Al termine dell'attività, vedrai gli oggetti del tuo bucket Google Cloud Storage nel tuo bucket S3.

Configurazione dei trasferimenti con Microsoft Azure Blob Storage

Con AWS DataSync, puoi trasferire dati tra Microsoft Azure Blob Storage (incluso l'archiviazione Azure Data Lake Storage Gen2 BLOB) e i seguenti servizi AWS di archiviazione:

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Per configurare questo tipo di trasferimento, crei una sede per il tuoAzure Blob Storage. È possibile utilizzare questa posizione come origine o destinazione del trasferimento. Un DataSync agente è necessario solo quando si trasferiscono dati tra Azure Blob e Amazon EFS o Amazon o quando si

utilizzano FSx attività in modalità Basic. Non è necessario un agente per trasferire dati tra Azure Blob e Amazon S3 usando la modalità Enhanced.

Fornire l'accesso al DataSync Azure Blob Storage

La modalità di DataSync accesso Azure Blob Storage dipende da diversi fattori, tra cui il trasferimento da o verso l'archiviazione BLOB e il tipo di token SAS (Shared Access Signature) che stai utilizzando. I tuoi oggetti devono inoltre trovarsi in un livello di accesso con cui sia DataSync possibile lavorare.

Argomenti

- Token SAS
- Livelli di accesso

Token SAS

Un token SAS specifica le autorizzazioni di accesso per l'archiviazione BLOB. (Per ulteriori informazioni su SAS, consulta la Azure Blob Storage documentazione.)

È possibile generare token SAS per fornire diversi livelli di accesso. DataSync supporta token con i seguenti livelli di accesso:

- Account
- Container

Le autorizzazioni di accesso DataSync necessarie dipendono dall'ambito del token. Se non disponi delle autorizzazioni corrette, il trasferimento potrebbe fallire. Ad esempio, il trasferimento non avrà esito positivo se sposti oggetti con tag Azure Blob Storage ma il token SAS non dispone delle autorizzazioni per i tag.

Argomenti

- Autorizzazioni del token SAS per l'accesso a livello di account
- Autorizzazioni del token SAS per l'accesso a livello di contenitore
- Politiche di scadenza SAS

Autorizzazioni del token SAS per l'accesso a livello di account

DataSync richiede un token di accesso a livello di account con le seguenti autorizzazioni (a seconda che si stia effettuando il trasferimento da o verso). Azure Blob Storage

Transfers from blob storage

- Servizi consentiti: Blob
- Tipi di risorse consentiti: contenitore, oggetto

  Se non includi queste autorizzazioni, non DataSync puoi trasferire i metadati degli oggetti, inclusi i tag degli oggetti.
- Autorizzazioni consentite: lettura, elenco
- Autorizzazioni consentite per l'indice BLOB: lettura/scrittura (se si desidera DataSync copiare i tag degli oggetti)

Transfers to blob storage

- Servizi consentiti — Blob
- Tipi di risorse consentiti: contenitore, oggetto

  Se non includi queste autorizzazioni, non DataSync puoi trasferire i metadati degli oggetti, inclusi i tag degli oggetti.
- Autorizzazioni consentite: lettura, scrittura, elenco, eliminazione (se desideri DataSync rimuovere file che non sono nella fonte di trasferimento)
- Autorizzazioni consentite per l'indice BLOB: lettura/scrittura (se desideri DataSync copiare i tag degli oggetti)

Autorizzazioni del token SAS per l'accesso a livello di contenitore

DataSync necessita di un token di accesso a livello di contenitore con le seguenti autorizzazioni (a seconda che si stia effettuando il trasferimento da o verso). Azure Blob Storage

Transfers from blob storage

- Lettura
- Elenco

- Tag (se desideri DataSync copiare i tag degli oggetti)

> **Note**
>
> Non è possibile aggiungere l'autorizzazione al tag quando si genera un token SAS nel Azure portale. Per aggiungere l'autorizzazione al tag, genera invece il token utilizzando l'Azure Storage Explorerapp o genera un token SAS che fornisca l'accesso a livello di account.

Transfers to blob storage

- Lettura
- Scrittura
- Elenco
- Elimina (se desideri DataSync rimuovere file che non sono nella fonte di trasferimento)
- Tag (se vuoi copiare DataSync i tag degli oggetti)

> **Note**
>
> Non è possibile aggiungere l'autorizzazione al tag quando si genera un token SAS nel Azure portale. Per aggiungere l'autorizzazione al tag, genera invece il token utilizzando l'Azure Storage Explorerapp o genera un token SAS che fornisca l'accesso a livello di account.

Politiche di scadenza SAS

Assicurati che il tuo SAS non scada prima di completare il trasferimento. Per informazioni sulla configurazione di una politica di scadenza SAS, consulta la Azure Blob Storage documentazione.

Se il SAS scade durante il trasferimento, non DataSync può più accedere alla tua Azure Blob Storage posizione. (È possibile che venga visualizzato un errore Failed to open directory). In tal caso, aggiorna la tua posizione con un nuovo token SAS e riavvia l' DataSync attività.

Livelli di accesso

Durante il trasferimento daAzure Blob Storage, DataSync può copiare oggetti nei livelli «caldo» e «freddo». Per gli oggetti nel livello di accesso all'archivio, è necessario reidratarli sul livello «caldo» o «freddo» prima di poterli copiare.

Durante il trasferimento suAzure Blob Storage, è DataSync possibile copiare gli oggetti nei livelli di accesso «caldo», «freddo» e «archivio». Se stai copiando oggetti nel livello di accesso all'archivio, non DataSync puoi verificare il trasferimento se stai cercando di verificare tutti i dati nella destinazione.

DataSync non supporta il livello di accesso a freddo. Per ulteriori informazioni sui livelli di accesso, consulta la Azure Blob Storagedocumentazione.

Considerazioni sui trasferimenti Azure Blob Storage

Quando si pianifica di trasferire dati da Azure Blob Storage o verso DataSync, è necessario tenere presenti alcuni aspetti.

Argomenti

- Costi
- Tipi di BLOB
- DisponibilitàRegione AWS
- Copiare i tag degli oggetti
- Trasferimento su Amazon S3
- Eliminazione delle directory in una destinazione di trasferimento
- Limitazioni

Costi

Le tariffe associate allo spostamento o all'uscita dei dati Azure Blob Storage possono includere:

- Esecuzione di una macchina Azure virtuale (VM) (se si implementa un DataSync agente) Azure
- Esecuzione di un' EC2istanza Amazon (se distribuisci un DataSync agente in un AWS VPC interno)
- Trasferimento dei dati tramite utilizzo DataSync, inclusi i costi di richiesta relativi ad Azure Blob StorageAmazon S3 (se S3 è una delle tue sedi di trasferimento)

- Trasferimento di dati in entrata o in uscita da Azure Blob Storage
- Archiviazione dei dati in un servizio AWS di archiviazione supportato da DataSync

Tipi di BLOB

Il DataSync funzionamento dei tipi di blob dipende dal fatto che il trasferimento venga effettuato o meno. Azure Blob Storage Quando sposti i dati nell'archivio blob, gli oggetti o i file che DataSync trasferisci possono essere solo blob a blocchi. Quando sposti i dati dall'archivio BLOB, DataSync puoi trasferire blocchi, pagine e aggiungere BLOB.

Per ulteriori informazioni sui tipi di blob, consulta la documentazione. Azure Blob Storage

DisponibilitàRegione AWS

Puoi creare una posizione di Azure Blob Storage trasferimento in qualsiasi Regione AWS posizione supportata da DataSync.

Copiare i tag degli oggetti

La possibilità di DataSync conservare i tag degli oggetti durante il trasferimento da o verso l'oggetto Azure Blob Storage dipende dai seguenti fattori:

- La dimensione dei tag di un oggetto: non è DataSync possibile trasferire un oggetto con tag che superano i 2 KB.
- Se DataSync è configurato per copiare i tag degli oggetti: per impostazione predefinita, DataSync copia i tag degli oggetti.
- Lo spazio dei nomi utilizzato dall'account di Azure archiviazione: DataSync può copiare i tag degli oggetti se l'account di Azure archiviazione utilizza uno spazio dei nomi semplice, ma non se l'account utilizza uno spazio dei nomi gerarchico (una funzionalità di). Azure Data Lake Storage Gen2 L' DataSync operazione avrà esito negativo se si tenta di copiare i tag degli oggetti e l'account di archiviazione utilizza uno spazio dei nomi gerarchico.
- Se il token SAS autorizza l'etichettatura: le autorizzazioni necessarie per copiare i tag degli oggetti variano a seconda del livello di accesso fornito dal token. La tua attività fallirà se provi a copiare i tag degli oggetti e il tuo token non dispone delle autorizzazioni giuste per l'etichettatura. Per ulteriori informazioni, consulta i requisiti di autorizzazione per i token di accesso a livello di account o i token di accesso a livello di contenitore.

Trasferimento su Amazon S3

Durante il trasferimento su Amazon S3 DataSync , non Azure Blob Storage trasferirà oggetti più grandi di 5 TB o oggetti con metadati più grandi di 2 KB.

Eliminazione delle directory in una destinazione di trasferimento

Durante il trasferimento suAzure Blob Storage, DataSync è possibile rimuovere oggetti nell'archivio BLOB che non sono presenti nella fonte di trasferimento. (Puoi configurare questa opzione cancellando l'impostazione Mantieni i file eliminati nella console. DataSync Il token SAS deve inoltre disporre delle autorizzazioni di eliminazione.)

Quando configuri il trasferimento in questo modo, DataSync non eliminerà le directory nell'archivio BLOB se l'account di archiviazione utilizza uno Azure spazio dei nomi gerarchico. In questo caso, è necessario eliminare manualmente le directory (ad esempio, utilizzando). Azure Storage Explorer

Limitazioni

Ricorda le seguenti limitazioni quando trasferisci dati da o verso: Azure Blob Storage

- DataSync crea alcune directory in una posizione per facilitare il trasferimento. Se si Azure Blob Storage tratta di una posizione di destinazione e l'account di archiviazione utilizza uno spazio dei nomi gerarchico, è possibile che nella cartella siano presenti sottodirectory specifiche per le attività (ad esempio). `task-000011112222abcde` `/.aws-datasync` DataSync in genere elimina queste sottodirectory dopo un trasferimento. Se ciò non accade, puoi eliminare tu stesso queste directory specifiche delle attività purché un'attività non sia in esecuzione.
- DataSync non supporta l'utilizzo di un token SAS per accedere solo a una cartella specifica nel contenitore. Azure Blob Storage
- Non è possibile fornire DataSync un token SAS di delega utente per accedere allo storage blob.

Creazione del tuo DataSync agente (opzionale)

Un DataSync agente è necessario solo quando si trasferiscono dati tra Azure Blob e Amazon EFS o Amazon o quando si utilizzano FSx attività in modalità Basic. Non è necessario un agente per trasferire dati tra Azure Blob e Amazon S3 usando la modalità Enhanced. Questa sezione descrive come distribuire e attivare un agente.

> **Tip**
>
> Sebbene sia possibile distribuire il proprio agente su un' EC2 istanza Amazon, l'utilizzo di un Microsoft Hyper-V agente potrebbe comportare una riduzione della latenza di rete e una maggiore compressione dei dati.

Agenti Microsoft Hyper-V

Puoi distribuire il tuo DataSync agente direttamente all'interno Azure di un'immagine. Microsoft Hyper-V

> **Tip**
>
> Prima di continuare, valuta la possibilità di utilizzare uno script di shell che possa aiutarti a distribuire l'agente Hyper-V più rapidamente. Azure Puoi ottenere ulteriori informazioni e scaricare il codice su. GitHub
> Se usi lo script, puoi passare alla sezione relativaOttenere la chiave di attivazione del tuo agente.

Argomenti

- Prerequisiti
- Scaricamento e preparazione del tuo agente
- Implementazione del tuo agente in Azure
- Ottenere la chiave di attivazione del tuo agente
- Attivazione del tuo agente

Prerequisiti

Per preparare l' DataSync agente e distribuirloAzure, è necessario effettuare le seguenti operazioni:

- Abilita Hyper-V sul tuo computer locale.
- Installa PowerShell(incluso ilHyper-V Module).
- Installa la AzureCLI.

- Installare AzCopy.

Scaricamento e preparazione del tuo agente

Scarica un agente dalla DataSync console. Prima di poter implementare l'agenteAzure, è necessario convertirlo in un disco rigido virtuale (VHD) di dimensioni fisse. Per ulteriori informazioni, consulta la documentazione relativa ad Azure.

Per scaricare e preparare l'agente

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Agenti, quindi scegli Crea agente.
3. Per Hypervisor, scegli Microsoft Hyper-V, quindi scegli Scarica l'immagine.

   L'agente scarica un `.zip` file che contiene un `.vhdx` file.
4. Estrai il `.vhdx` file sul tuo computer locale.
5. Aprire PowerShell e procedere come segue:

   a. Copiare il seguente `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. Sostituisci ogni istanza di *`local-path-to-vhdx-file`* con la posizione del `.vhdx` file sul computer locale.

   c. Esegui il comando .

   Il tuo agente è ora un VHD a dimensione fissa (con un formato di `.vhd` file) pronto per la distribuzione. Azure

Implementazione del tuo agente in Azure

Il dispiegamento del tuo DataSync agente implica: Azure

- La creazione di un disco gestito in Azure
- Caricamento del tuo agente su quel disco gestito

- Collegamento del disco gestito a una macchina virtuale Linux

Per distribuire il tuo agente in Azure

1. InPowerShell, vai alla directory che contiene il `.vhd` file del tuo agente.
2. Esegui il `ls` comando e salva il `Length` valore (ad esempio,`85899346432`).

   Questa è la dimensione in byte dell'immagine dell'agente, necessaria per creare un disco gestito in grado di contenere l'immagine.
3. Effettuate le seguenti operazioni per creare un disco gestito:

   a. Copia il seguente Azure comando CLI:

   ```
   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*Sostituiscilo con un nome per il tuo disco gestito.

   c. Sostituiscilo *your-resource-group* con il nome del gruppo di Azure risorse a cui appartiene l'account di archiviazione.

   d. Sostituiscilo *your-azure-region* con la Azure regione in cui si trova il tuo gruppo di risorse.

   e. Sostituiscila *agent-size-bytes* con la dimensione dell'immagine dell'agente.

   f. Esegui il comando .

   Questo comando crea un disco gestito vuoto con uno SKU standard in cui puoi caricare il tuo DataSync agente.
4. Per generare una firma ad accesso condiviso (SAS) che consenta l'accesso in scrittura al disco gestito, procedi come segue:

   a. Copia il seguente Azure comando CLI:

   ```
   az disk grant-access -n your-managed-disk `
   -g your-resource-group `
   ```

```
--access-level Write `
--duration-in-seconds 86400
```

b. Sostituisci *your-managed-disk* con il nome del disco gestito che hai creato.

c. Sostituisci *your-resource-group* con il nome del gruppo di Azure risorse a cui appartiene l'account di archiviazione.

d. Esegui il comando .

Nell'output, prendi nota dell'URI SAS. È necessario questo URI quando si carica l'agente suAzure.

Il SAS consente di scrivere sul disco per un massimo di un'ora. Ciò significa che hai un'ora per caricare il tuo agente sul disco gestito.

5. Per caricare il tuo agente sul tuo disco gestito inAzure, procedi come segue:

a. Copia il seguente `AzCopy` comando:

```
.\azcopy copy local-path-to-vhd-file sas-uri --blob-type PageBlob
```

b. Sostituisci *local-path-to-vhd-file* con la posizione del `.vhd` file dell'agente sul tuo computer locale.

c. Sostituisci *sas-uri* con l'URI SAS che hai ottenuto quando hai eseguito il `az disk grant-access` comando.

d. Esegui il comando .

6. Al termine del caricamento dell'agente, revoca l'accesso al disco gestito. Per fare ciò, copia il seguente comando Azure CLI:

```
az disk revoke-access -n your-managed-disk -g your-resource-group
```

a. Sostituiscilo *your-resource-group* con il nome del gruppo di Azure risorse a cui appartiene l'account di archiviazione.

b. Sostituisci *your-managed-disk* con il nome del disco gestito che hai creato.

c. Esegui il comando .

7. Effettua le seguenti operazioni per collegare il disco gestito a una nuova macchina Linux virtuale:

a. Copia il seguente Azure comando CLI:

```
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. Sostituiscilo *your-resource-group* con il nome del gruppo di Azure risorse a cui appartiene l'account di archiviazione.

c. Sostituiscila *your-agent-vm* con un nome per la macchina virtuale che ricordi.

d. Sostituisci *your-managed-disk* con il nome del disco gestito che stai collegando alla macchina virtuale.

e. Esegui il comando .

Hai implementato il tuo agente. Prima di iniziare a configurare il trasferimento dei dati, è necessario attivare l'agente.

Ottenere la chiave di attivazione del tuo agente

Per ottenere manualmente la chiave di attivazione del tuo DataSync agente, segui questi passaggi.

In alternativa, DataSync puoi ottenere automaticamente la chiave di attivazione, ma questo approccio richiede una certa configurazione di rete.

Per ottenere la chiave di attivazione del tuo agente

1. Nel Azure portale, abilita la diagnostica di avvio per la macchina virtuale per il tuo agente scegliendo l'impostazione Abilita con account di archiviazione personalizzato e specificando il tuo Azure account di archiviazione.

   Dopo aver abilitato la diagnostica di avvio per la macchina virtuale dell'agente, puoi accedere alla console locale dell'agente per ottenere la chiave di attivazione.
2. Mentre sei ancora nel Azure portale, vai alla tua macchina virtuale e scegli Console seriale.
3. Nella console locale dell'agente, accedi utilizzando le seguenti credenziali predefinite:

   - Username (Nome utente – **admin**
   - Password: **password**

A un certo punto consigliamo di modificare almeno la password dell'agente. Nella console locale dell'agente, **5** accedi al menu principale, quindi usa il `passwd` comando per modificare la password.

4. Inserisci **0** per ottenere la chiave di attivazione dell'agente.
5. Inserisci il Regione AWS luogo in cui stai utilizzando DataSync (ad esempio,**us-east-1**).
6. Scegli l'endpoint del servizio con cui l'agente utilizzerà per connettersi AWS.
7. Salva il valore dell'`Activation key`output.

Attivazione del tuo agente

Dopo aver ottenuto la chiave di attivazione, puoi completare la creazione del tuo DataSync agente.

Per attivare l'agente

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Agenti, quindi scegli Crea agente.
3. Per Hypervisor, scegli. Microsoft Hyper-V
4. Per Tipo di endpoint, scegli lo stesso tipo di endpoint di servizio che hai specificato quando hai ricevuto la chiave di attivazione dell'agente (ad esempio, scegli Endpoint di servizio pubblico in). *`Region name`*
5. Configura la rete in modo che funzioni con il tipo di endpoint di servizio utilizzato dall'agente. Per i requisiti di rete degli endpoint di servizio, consulta i seguenti argomenti:
   - Endpoint VPC
   - Endpoint pubblici
   - Endpoint FIPS (Federal Information Processing Standard)
6. Per la chiave di attivazione, procedi come segue:
   a. Scegli Inserisci manualmente la chiave di attivazione del tuo agente.
   b. Inserisci la chiave di attivazione che hai ricevuto dalla console locale dell'agente.
7. Scegliere Create agent (Crea agente).

Il tuo agente è pronto a connettersi con il tuoAzure Blob Storage. Per ulteriori informazioni, consulta Creazione della località Azure Blob Storage di trasferimento.

EC2 Agenti Amazon

Puoi distribuire il tuo DataSync agente su un' EC2 istanza Amazon.

Per creare un EC2 agente Amazon

1. Implementa un EC2 agente Amazon.
2. Scegli un endpoint di servizio con cui l'agente comunica. AWS

   In questa situazione, consigliamo di utilizzare un endpoint del servizio Virtual Private Cloud (VPC).
3. Configura la tua rete per funzionare con gli endpoint del servizio VPC.
4. Attiva l'agente.

Creazione della località Azure Blob Storage di trasferimento

È possibile DataSync configurare l'utilizzo del proprio Azure Blob Storage come fonte o destinazione di trasferimento.

Prima di iniziare

Assicurati di sapere come DataSync accede Azure Blob Storage e funziona con i livelli di accesso e i tipi di blob. È inoltre necessario un DataSync agente in grado di connettersi al contenitore. Azure Blob Storage

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per Tipo di posizione, scegliere Microsoft Azure Blob Storage.
4. Per Container URL, inserisci l'URL del contenitore coinvolto nel trasferimento.
5. (Facoltativo) Per il livello di accesso, se utilizzato come destinazione, scegli il livello di accesso in cui desideri trasferire i tuoi oggetti o file.
6. Per Cartella, inserisci i segmenti di percorso se desideri limitare il trasferimento a una directory virtuale del contenitore (ad esempio,`/my/images`).
7. Se il trasferimento richiede un agente, scegli Usa agenti, quindi scegli l' DataSync agente che può connettersi al tuo Azure Blob Storage contenitore.

8. Per il token SAS, fornisci le credenziali necessarie per accedere DataSync al tuo archivio BLOB. Alcuni set di dati pubblici sull'archiviazione BLOB di Azure non richiedono credenziali. È possibile inserire direttamente un token SAS o specificare un AWS Secrets Manager segreto che contenga il token. Per ulteriori informazioni, vedere Fornitura di credenziali per le posizioni di archiviazione.

   Il token SAS fa parte della stringa URI SAS che segue l'URI della risorsa di archiviazione e un punto interrogativo (?). Un token ha un aspetto simile al seguente:

   ```
   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. (Facoltativo) Immettete i valori nei campi Chiave e Valore per etichettare la posizione.

   I tag ti aiutano a gestire, filtrare e cercare AWS le tue risorse. È consigliabile creare almeno un tag di nome per la posizione.

10. Scegli Crea posizione.

Usando il AWS CLI

1. Copia il seguente `create-location-azure-blob` comando:

   ```
   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. Per il `--container-url` parametro, specifica l'URL del Azure Blob Storage contenitore coinvolto nel trasferimento.
3. Per il parametro `--authentication-type`, specifica `SAS`. Se stai accedendo a un set di dati pubblico che non richiede l'autenticazione, specifica`NONE`.
4. Per l'`Token`opzione del `--sas-configuration` parametro, specifica il token SAS che consente di accedere DataSync al tuo archivio BLOB.

Puoi anche fornire parametri aggiuntivi per proteggere le tue chiavi utilizzando. AWS Secrets Manager Per ulteriori informazioni, vedere Fornitura di credenziali per le posizioni di archiviazione.

Il token SAS fa parte della stringa URI SAS che segue l'URI della risorsa di archiviazione e un punto interrogativo (?). Un token ha un aspetto simile al seguente:

```
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. (Facoltativo) Per il `--agent-arns` parametro, specifica l'Amazon Resource Name (ARN) dell' DataSync agente che può connettersi al tuo contenitore.

   Ecco un esempio di ARN dell'agente: `arn:aws:datasync:`*`us-east-1`*`:`*`123456789012`*`:agent/agent-`*`01234567890aaabfb`*

   È possibile specificare più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .
6. Per il `--subdirectory` parametro, specificate i segmenti di percorso se desiderate limitare il trasferimento a una directory virtuale del contenitore (ad esempio,`/my/images`).
7. (Facoltativo) Per il `--access-tier` parametro, specificate il livello di accesso (`HOTCOOL`, o`ARCHIVE`) in cui desiderate trasferire gli oggetti o i file.

   Questo parametro si applica solo quando si utilizza questa posizione come destinazione di trasferimento.
8. (Facoltativo) Per il `--tags` parametro, specificate le coppie chiave-valore che possono aiutarvi a gestire, filtrare e cercare la vostra posizione.

   È consigliabile creare un tag di nome per la posizione.
9. Esegui il comando `create-location-azure-blob`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN della posizione creata. Per esempio:

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh"
}
```

Visualizzazione della località di Azure Blob Storage trasferimento

Puoi ottenere dettagli sulla località di DataSync trasferimento esistente per il tuoAzure Blob Storage.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.
3. Scegli la tua Azure Blob Storage posizione.

   Puoi visualizzare i dettagli sulla tua posizione, incluse le attività di DataSync trasferimento che la utilizzano.

Utilizzando il AWS CLI

1. Copia il seguente `describe-location-azure-blob` comando:

   ```
   aws datasync describe-location-azure-blob \
     --location-arn "your-azure-blob-location-arn"
   ```

2. Per il `--location-arn` parametro, specificate l'ARN per la Azure Blob Storage posizione che avete creato (ad esempio,`arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Esegui il comando `describe-location-azure-blob`.

   Riceverai una risposta che mostra i dettagli sulla tua posizione. Per esempio:

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

Aggiornamento della località Azure Blob Storage di trasferimento

Se necessario, puoi modificare la configurazione della tua posizione nella console o utilizzando il AWS CLI.

Utilizzando il AWS CLI

1. Copia il seguente `update-location-azure-blob` comando:

```
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. Per il `--location-arn` parametro, specifica l'ARN per la Azure Blob Storage posizione che stai aggiornando (ad esempio,`arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Per il parametro `--authentication-type`, specifica `SAS`.
4. Per l'`Token`opzione del `--sas-configuration` parametro, specifica il token SAS che consente di accedere DataSync al tuo archivio BLOB.

   Il token fa parte della stringa URI SAS che segue l'URI della risorsa di archiviazione e un punto interrogativo (?). Un token ha un aspetto simile al seguente:

```
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. Per il `--agent-arns` parametro, specifica l'Amazon Resource Name (ARN) dell' DataSync agente che desideri connettere al tuo contenitore.

   Ecco un esempio di ARN dell'agente: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

   È possibile specificare più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti DataSync .

6. Per il `--subdirectory` parametro, specificate i segmenti di percorso se desiderate limitare il trasferimento a una directory virtuale del contenitore (ad esempio,`/my/images`).
7. (Facoltativo) Per il `--access-tier` parametro, specificate il livello di accesso (`HOTCOOL`, o`ARCHIVE`) in cui desiderate trasferire gli oggetti.

   Questo parametro si applica solo quando si utilizza questa posizione come destinazione di trasferimento.

Passaggi successivi

Dopo aver creato una DataSync posizione per la tuaAzure Blob Storage, puoi continuare a configurare il trasferimento. Ecco alcuni passaggi successivi da considerare:

1. Se non l'hai già fatto, crea un'altra posizione in cui intendi trasferire i tuoi dati da o verso il tuoAzure Blob Storage.
2. Scopri come DataSync gestisce i metadati e i file speciali, in particolare se le località di trasferimento non hanno una struttura di metadati simile.
3. Configura il modo in cui i tuoi dati vengono trasferiti. Ad esempio, puoi trasferire solo un sottoinsieme di dati o eliminare file nell'archivio BLOB che non si trovano nella posizione di origine (purché il token SAS disponga delle autorizzazioni di eliminazione).
4. Inizia il trasferimento.

Configurazione dei AWS DataSync trasferimenti con Microsoft Azure Files Condivisioni SMB

È possibile configurare il trasferimento AWS DataSync di dati da o verso un Microsoft Azure Files Condivisione Server Message Block (SMB).

> **Tip**
>
> Per una procedura dettagliata sullo spostamento dei dati dalle condivisioni SMB di Azure Files a AWS, consulta lo Storage Blog.AWS

Fornire DataSync l'accesso alle condivisioni SMB

DataSync si connette alla condivisione SMB utilizzando il protocollo SMB e si autentica con le credenziali fornite dall'utente.

Argomenti

- Versioni del protocollo SMB supportate
- Autorizzazioni richieste

Versioni del protocollo SMB supportate

Per impostazione predefinita, sceglie DataSync automaticamente una versione del protocollo SMB in base alla negoziazione con il file server SMB.

Puoi anche configurare l'utilizzo DataSync di una versione SMB specifica, ma ti consigliamo di farlo solo se hai problemi a negoziare automaticamente con DataSync il file server SMB. DataSync supporta le versioni SMB 1.0 e successive. Per motivi di sicurezza, consigliamo di utilizzare la versione 3.0.2 o successiva di SMB. Le versioni precedenti, come SMB 1.0, contengono vulnerabilità di sicurezza note che gli aggressori possono sfruttare per compromettere i dati.

Consulta la tabella seguente per un elenco delle opzioni disponibili nella console e nell'API: DataSync

Opzione Console	Opzione API	Descrizione
Automatica	`AUTOMATIC`	DataSync e il file server SMB negoziano la versione più recente di SMB che supportano reciprocamente tra la 2.1 e la 3.1.1. Questa è l'opzione predefinita e consigliata. Se scegli una versione specifica che il tuo server di file non supporta, potresti ricevere un errore `Operation Not Supported` .
SMB 3.0.2	`SMB3`	Limita la negoziazione del protocollo alla sola versione SMB 3.0.2.
SMB 2.1	`SMB2`	Limita la negoziazione del protocollo alla sola versione 2.1 di SMB.

Opzione Console	Opzione API	Descrizione
SMB 2.0	`SMB2_0`	Limita la negoziazione del protocollo solo alla versione 2.0 di SMB.
SMB 1.0	`SMB1`	Limita la negoziazione del protocollo solo alla versione 1.0 di SMB.

Autorizzazioni richieste

DataSync necessita di un utente con il permesso di montare e accedere alla tua posizione SMB. Può trattarsi di un utente locale sul file server Windows o di un utente di dominio definito in Microsoft Active Directory.

Per impostare la proprietà degli oggetti, è DataSync necessario il `SE_RESTORE_NAME` privilegio, che in genere viene concesso ai membri dei gruppi integrati di Active Directory Backup Operators e Domain Admins. L'assegnazione di questo privilegio DataSync a un utente consente inoltre di garantire autorizzazioni sufficienti per file, cartelle e metadati dei file, ad eccezione degli elenchi di controllo degli accessi al sistema NTFS (). SACLs

Per la copia sono necessari privilegi aggiuntivi. SACLs In particolare, ciò richiede il `SE_SECURITY_NAME` privilegio Windows, concesso ai membri del gruppo Domain Admins. Se configuri l'attività per la copia SACLs, assicurati che l'utente disponga dei privilegi richiesti. Per ulteriori informazioni sulla configurazione di un'attività da copiare SACLs, consulta. Configurazione della modalità di gestione di file, oggetti e metadati

Quando copi dati tra un file server SMB e il file system Amazon FSx for Windows File Server, le posizioni di origine e destinazione devono appartenere allo stesso dominio Microsoft Active Directory o avere una relazione di trust di Active Directory tra i rispettivi domini.

Creazione della posizione di trasferimento di Azure Files utilizzando la console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per Location type (Tipo di posizione), scegliere Server Message Block (SMB).

Sarà possibile configurare questa posizione come origine o destinazione in un secondo momento.

4. Per gli agenti, scegli uno o più DataSync agenti che desideri connettere alla tua condivisione SMB.

   Se scegli più di un agente, assicurati di aver compreso l'utilizzo di più agenti per una sede.

5. Per SMB Server, inserisci il nome o l'indirizzo IP del Domain Name System (DNS) della condivisione SMB che il tuo DataSync agente installerà.

   > **Note**
   >
   > Non è possibile specificare un indirizzo IP versione 6 ()IPv6.

6. Per Share name, inserisci il nome della condivisione esportata dalla tua condivisione SMB in cui DataSync leggerà o scriverà i dati.

   È possibile includere una sottodirectory nel percorso di condivisione (ad esempio,). `/path/to/subdirectory` Assicurati che anche altri client SMB della tua rete possano montare questo percorso.

   Per copiare tutti i dati nella sottodirectory, DataSync devi essere in grado di montare la condivisione SMB e accedere a tutti i suoi dati. Per ulteriori informazioni, consulta Autorizzazioni richieste.

7. (Facoltativo) Espandi le impostazioni aggiuntive e scegli una versione SMB DataSync da utilizzare per accedere alla condivisione SMB.

   Per impostazione predefinita, sceglie DataSync automaticamente una versione in base alla negoziazione con la condivisione SMB. Per informazioni, consultare Versioni SMB supportate.

8. Per Utente, inserisci un nome utente che possa montare la tua condivisione SMB e che disponga dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.

   Per ulteriori informazioni, consulta Autorizzazioni richieste.

9. Per Password, inserisci la password dell'utente che può montare la tua condivisione SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.

10. (Facoltativo) Per Dominio, inserisci il nome di dominio Windows a cui appartiene la tua condivisione SMB.

Se nel tuo ambiente sono presenti più domini, la configurazione di questa impostazione assicura che DataSync si connetta alla condivisione corretta.

11. (Facoltativo) Scegli Aggiungi tag per taggare la tua posizione.

    I tag sono coppie chiave-valore che ti aiutano a gestire, filtrare e cercare le tue sedi. È consigliabile creare almeno un tag di nome per la posizione.

12. Scegli Crea località.

Configurazione dei trasferimenti con altri archivi di oggetti nel cloud

Con AWS DataSync, puoi trasferire dati tra i servizi AWS di storage e i seguenti provider di cloud object storage:

- 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

Un DataSync agente è necessario solo quando si trasferiscono dati tra sistemi di storage in altri cloud e Amazon EFS o Amazon FSx o quando si utilizzano attività in modalità Basic. Non è necessario un agente per trasferire dati tra sistemi di storage in altri cloud e Amazon S3 utilizzando la modalità Enhanced.

Indipendentemente dal fatto che utilizzi un agente, devi anche creare una posizione di trasferimento per l'archiviazione di oggetti nel cloud (in particolare una posizione di archiviazione di oggetti). DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento.

Fornire DataSync l'accesso all'altro spazio di archiviazione di oggetti nel cloud

Il modo in cui DataSync accede allo storage di oggetti nel cloud dipende da diversi fattori, tra cui la compatibilità dello storage con l'API Amazon S3 e le autorizzazioni e le credenziali DataSync necessarie per accedere allo storage.

Argomenti

- Compatibilità con le API Amazon S3
- Autorizzazioni ed endpoint di archiviazione
- Credenziali di archiviazione

Compatibilità con le API Amazon S3

Il tuo storage di oggetti nel cloud deve essere compatibile con le seguenti operazioni dell'API Amazon S3 per DataSync poterti connettere:

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

Autorizzazioni ed endpoint di archiviazione

È necessario configurare le autorizzazioni che consentono di accedere DataSync all'archivio di oggetti nel cloud. Se il tuo object storage è una posizione di origine, DataSync necessita delle autorizzazioni di lettura ed elenco per il bucket da cui stai trasferendo i dati. Se l'object storage è una posizione di destinazione, sono necessarie DataSync le autorizzazioni di lettura, elenco, scrittura ed eliminazione per il bucket.

DataSync necessita inoltre di un endpoint (o server) per connettersi allo storage. La tabella seguente descrive gli endpoint che è DataSync possibile utilizzare per accedere ad altri archivi di oggetti nel cloud:

Altro provider di servizi cloud	Endpoint
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` (la maggior parte delle regioni)
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`

> **Important**
>
> Per dettagli su come configurare le autorizzazioni dei bucket e informazioni aggiornate sugli endpoint di archiviazione, consulta la documentazione del tuo provider di servizi cloud.

Credenziali di archiviazione

DataSync necessita inoltre delle credenziali per accedere al bucket di archiviazione degli oggetti coinvolto nel trasferimento. Potrebbe trattarsi di una chiave di accesso e una chiave segreta o qualcosa di simile a seconda del modo in cui il provider di archiviazione cloud fa riferimento a queste credenziali.

Per ulteriori informazioni, consulta la documentazione del tuo provider di servizi cloud.

Considerazioni relative al trasferimento da altri sistemi di archiviazione di oggetti nel cloud

Quando si pianifica di trasferire oggetti da o verso un altro provider di archiviazione cloud utilizzando DataSync, ci sono alcune cose da tenere a mente.

Argomenti

- Costi
- Classi di archiviazione
- Tag dell'oggetto
- Trasferimento su Amazon S3

Costi

Le tariffe associate allo spostamento dei dati da e verso un altro provider di cloud storage possono includere:

- Esecuzione di un' EC2istanza Amazon per il tuo DataSync agente
- Trasferimento dei dati tramite utilizzo DataSync, inclusi i costi di richiesta relativi allo storage di oggetti nel cloud e ad Amazon S3 (se S3 è la destinazione di trasferimento)
- Trasferimento di dati da o verso il tuo cloud storage (controlla i prezzi del tuo provider di servizi cloud)
- Archiviazione dei dati in un servizio AWS di archiviazione supportato da DataSync

- Archiviazione dei dati in un altro provider di servizi cloud (controlla i prezzi del tuo provider di servizi cloud)

Classi di archiviazione

Alcuni provider di cloud storage dispongono di classi di archiviazione (simili ad Amazon S3) che non DataSync possono essere lette senza prima essere ripristinate. Ad esempio, Oracle Cloud Infrastructure Object Storage ha una classe di archiviazione. È necessario ripristinare gli oggetti in quella classe di archiviazione prima di DataSync poterli trasferire. Per ulteriori informazioni, consulta la documentazione del tuo provider di servizi cloud.

Tag dell'oggetto

Non tutti i provider di servizi cloud supportano i tag degli oggetti. Quelli che lo fanno potrebbero non consentire l'interrogazione dei tag tramite l'API Amazon S3. In entrambe le situazioni, l'operazione di DataSync trasferimento potrebbe non riuscire se si tenta di copiare i tag degli oggetti.

È possibile evitare questo problema deselezionando la casella di controllo Copia i tag degli oggetti nella DataSync console durante la creazione, l'avvio o l'aggiornamento dell'attività.

Trasferimento su Amazon S3

Durante il trasferimento su Amazon S3 DataSync , non è possibile trasferire oggetti di dimensioni superiori a 5 TB. DataSyncinoltre, può copiare solo i metadati degli oggetti fino a 2 KB.

Creando il tuo agente DataSync

Un DataSync agente è necessario solo quando si trasferiscono dati tra sistemi di storage in altri cloud e Amazon EFS o Amazon FSx o quando si utilizzano attività in modalità Basic. Non è necessario un agente per trasferire dati tra sistemi di storage in altri cloud e Amazon S3 utilizzando la modalità Enhanced. Questa sezione descrive come distribuire e attivare un agente su un' EC2 istanza Amazon nel tuo cloud privato virtuale (VPC) in. AWS

Per creare un EC2 agente Amazon

1. Implementa un EC2 agente Amazon.
2. Scegli un endpoint di servizio con cui l'agente comunica. AWS

   In questa situazione, consigliamo di utilizzare un endpoint di servizio VPC.
3. Configura la tua rete per funzionare con gli endpoint del servizio VPC.

4. Attiva l'agente.

Creazione di una posizione di trasferimento per l'altro spazio di archiviazione di oggetti nel cloud

È possibile DataSync configurare l'utilizzo dello storage di oggetti nel cloud come posizione di origine o destinazione.

Prima di iniziare

Assicurati di sapere come DataSync accede al tuo archivio di oggetti nel cloud. È inoltre necessario un DataSync agente in grado di connettersi al cloud object storage.

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni e Crea posizione.
3. Per Tipo di posizione, scegli Archiviazione oggetti.
4. Per Server, inserisci l'endpoint che DataSync puoi utilizzare per accedere al tuo archivio di oggetti nel cloud:
   - 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` (la maggior parte delle regioni)
   - 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. Per Bucket name, inserisci il nome del bucket di archiviazione degli oggetti verso o da cui stai trasferendo i dati.
6. Per Cartella, inserisci il prefisso di un oggetto. DataSync trasferisce solo oggetti con questo prefisso.

7. Se il trasferimento richiede un agente, scegli Usa agenti, quindi scegli l' DataSync agente che può connettersi al tuo cloud object storage.
8. Espandere Additional settings (Impostazioni aggiuntive). Per il protocollo Server, scegli HTTPS. Per Porta server, scegli 443.
9. Scorri verso il basso fino alla sezione Autenticazione. Assicurati che la casella di controllo Richiede credenziali sia selezionata, quindi fornisci DataSync le credenziali di archiviazione.
   - Per la chiave di accesso, inserisci l'ID per accedere al tuo archivio di oggetti nel cloud.
   - Per Chiave segreta, fornisci la chiave segreta per accedere al tuo archivio di oggetti nel cloud. Puoi inserire la chiave direttamente o specificare un AWS Secrets Manager segreto che contenga la chiave. Per ulteriori informazioni, vedere Fornitura di credenziali per le posizioni di archiviazione.
10. (Facoltativo) Immettete i valori nei campi Chiave e Valore per etichettare la posizione.

    I tag ti aiutano a gestire, filtrare e cercare AWS le tue risorse. È consigliabile creare almeno un tag di nome per la posizione.
11. Scegli Crea posizione.

Passaggi successivi

Dopo aver creato una DataSync posizione per l'archiviazione degli oggetti nel cloud, puoi continuare a configurare il trasferimento. Ecco alcuni passaggi successivi da considerare:

1. Se non l'hai già fatto, crea un'altra posizione in cui intendi trasferire i dati da o verso l'interno AWS.
2. Scopri come DataSync gestisce i metadati e i file speciali per le posizioni di archiviazione degli oggetti.
3. Configura il modo in cui i tuoi dati vengono trasferiti. Ad esempio, forse desideri trasferire solo un sottoinsieme dei tuoi dati.

   > **Important**
   >
   > Assicurati di configurare la modalità di DataSync copia corretta dei tag degli oggetti. Per ulteriori informazioni, consulta Considerazioni sui tag degli oggetti.

4. Inizia il trasferimento.

Trasferimento da o verso uno storage compatibile con S3 su Snowball Edge

Con AWS DataSync, puoi trasferire oggetti tra lo storage compatibile con Amazon S3 su un AWS Snowball Edge dispositivo o un cluster e uno dei seguenti servizi di AWS storage:

- Amazon S3
- Amazon Elastic File System (Amazon EFS)
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Prerequisiti

Prima di iniziare, assicurati di aver fatto quanto segue:

- Hai creato una risorsa AWS di archiviazione nel Regione AWS luogo in cui intendi trasferire i dati da o verso. Ad esempio, potrebbe trattarsi di un bucket S3 o di un file system Amazon EFS negli Stati Uniti orientali (Virginia settentrionale).
- È stata stabilita una connessione WAN (Wide Area Network) per il traffico in entrata e in uscita dall'ambiente di storage locale. Ad esempio, è possibile stabilire questo tipo di connessione con. AWS Direct Connect

  Quando crei il tuo DataSync agente, configurerai questa connessione WAN in modo che DataSync possa trasferire dati tra lo storage compatibile con Amazon S3 che è locale e la tua risorsa di storage in. AWS
- Scaricato e installato il client Snowball Edge.

Fornire DataSync l'accesso allo storage compatibile con S3

Per accedere al tuo bucket di storage compatibile con Amazon S3, è DataSync necessario quanto segue:

- Credenziali utente sul dispositivo o sul cluster Snowball Edge che possono accedere al bucket verso il quale o dal quale trasferisci i dati.
- Un certificato HTTPS che consente di DataSync verificare l'autenticità della connessione tra l' DataSync agente e l'`s3api`endpoint sul dispositivo o sul cluster.

Argomenti

- Ottenere le credenziali utente per accedere al bucket S3
- Ottenere un certificato per la connessione all's3apiendpoint

Ottenere le credenziali utente per accedere al bucket S3

DataSync richiede la chiave di accesso e la chiave segreta per un utente che può accedere al bucket con cui stai lavorando sul tuo dispositivo o cluster Snowball Edge.

Per ottenere le credenziali utente per accedere al tuo bucket

1. Apri un terminale ed esegui il client Snowball Edge.

   Per ulteriori informazioni sull'esecuzione del client Snowball Edge, consulta Using the Snowball Edge client nella Developer Guide.AWS Snowball Edge
2. Per ottenere le chiavi di accesso associate al dispositivo o al cluster, esegui il comando seguente: `snowballEdge`

   ```
   snowballEdge list-access-keys
   ```
3. Nell'output, individua la chiave di accesso per il bucket con cui DataSync funzionerà (ad esempio,`AKIAIOSFODNN7EXAMPLE`).
4. Per ottenere la chiave di accesso segreta, esegui il `snowballEdge` comando seguente. Sostituiscila *`access-key-for-datasync`* con la chiave di accesso che hai trovato nel passaggio precedente.

   ```
   snowballEdge get-secret-access-key --access-key-id access-key-for-datasync
   ```

   L'output include la chiave segreta corrispondente alla chiave di accesso (ad esempio,`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`).
5. Salva la chiave di accesso e la chiave segreta in un posto facile da ricordare.

Avrai bisogno di queste chiavi quando configurerai la posizione di DataSync origine per il trasferimento.

Ottenere un certificato per la connessione all'**s3api**endpoint

È necessario un certificato HTTPS in grado di verificare l'autenticità della connessione tra l' DataSync agente e un `s3api` endpoint sul dispositivo o sul cluster Snowball Edge.

Per ottenere un certificato per la connessione all'endpoint **`s3api`**

1. Nel client Snowball Edge, esegui il comando seguente: `list-certificates`

   ```
   snowballEdge list-certificates
   ```

   Nell'output, prendi nota del `CertificateArn` valore. Si tratta dell'Amazon Resource Name (ARN) del certificato. È necessario l'ARN per ottenere il contenuto del certificato.

2. Esegui il `get-certificate` comando seguente che specifica l'ARN del certificato che hai appena recuperato:

   ```
   snowballEdge get-certificate --certificate-arn arn:aws:snowball-
   device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
   ```

3. Copia l'output, comprese le `END CERTIFICATE` righe `BEGIN CERTIFICATE` e, e salvalo come file. `.pem`

   Esempio di **`get-certificate`** output:

   ```
   -----BEGIN CERTIFICATE-----
   Certificate
   -----END CERTIFICATE-----
   ```

Specificate questo `.pem` file quando create la posizione di DataSync origine per il trasferimento.

Creazione di un DataSync agente nell'ambiente di archiviazione locale

Durante un trasferimento, DataSync utilizza un agente per leggere o scrivere sullo storage compatibile con Amazon S3 sul dispositivo o sul cluster Snowball Edge.

Questo agente deve essere distribuito nell'ambiente di storage locale, dove può connettersi al dispositivo o al cluster tramite la rete. Ad esempio, è possibile eseguire l'agente su un VMware ESXi hypervisor con accesso alla rete locale al cluster.

Per creare un DataSync agente nell'ambiente di storage locale

1. Assicurati che l'DataSync agente possa essere eseguito sul tuo hypervisor e di allocargli abbastanza risorse per le macchine virtuali (VM).
2. Implementa l'agente nel tuo ambiente locale.

   Per istruzioni, consulta uno dei seguenti argomenti, a seconda del tipo di hypervisor su cui stai distribuendo l'agente:

   - Implementa il tuo agente su VMware
   - Implementa il tuo agente su una macchina basata su kernel Linux (KVM)
   - Implementa il tuo agente su Microsoft Hyper-V
   - Implementa il tuo agente su Amazon EC2

   > **Warning**
   >
   > Non è consigliabile distribuire un agente su Amazon EC2 Agent per accedere allo storage locale a causa della maggiore latenza di rete.

3. Configura la tua rete per consentire il seguente traffico tra l'agente e lo storage compatibile con Amazon S3:

Da	Per	Protocollo e porta
DataSync agente	Un'interfaccia di rete virtuale (VNI) per un `s3api` endpoint sul dispositivo o sul cluster. Se disponi di un cluster, può essere un qualsiasi `s3api` endpoint VNI.	TCP 443 (HTTPS)

   Se hai bisogno di trovare un VNI sul tuo dispositivo o cluster, consulta la descrizione delle interfacce di rete virtuali su Snowball Edge.

4. Scegli un endpoint del servizio che l'agente utilizza per comunicare con il servizio. DataSync
5. Attiva il tuo agente.

Configurazione della posizione di origine per il trasferimento

Dopo aver creato l'agente, puoi configurare la posizione di origine per il DataSync trasferimento.

> **Note**
>
> Le seguenti istruzioni presuppongono che tu stia effettuando il trasferimento da uno storage compatibile con Amazon S3, ma puoi anche utilizzare questa posizione come destinazione di trasferimento.

Per configurare la posizione di origine utilizzando la console DataSync

1. Aprire la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati. Scegli Attività, quindi scegli Crea attività.
3. Nella pagina Configure source location (Configura posizione di origine), scegliere Create a new location (Crea una nuova posizione).
4. Per Tipo di posizione, scegli Archiviazione oggetti.
5. Per gli agenti, scegli l' DataSync agente che hai creato nel tuo ambiente di storage locale.
6. Per Server, inserisci il VNI per l'`s3api`endpoint utilizzato dallo storage compatibile con Amazon S3.

   Se disponi di un cluster Snowball Edge anziché di un singolo dispositivo, puoi specificare qualsiasi endpoint del `s3api` cluster. VNIs
7. Per Bucket name, inserisci il nome del bucket di storage compatibile con Amazon S3 da cui stai trasferendo gli oggetti.
8. Per Folder, inserisci il prefisso di un oggetto.

   DataSync trasferisce solo oggetti con questo prefisso.
9. Per configurare la DataSync connessione al dispositivo o al cluster Snowball Edge, espandi Impostazioni aggiuntive ed esegui le seguenti operazioni:

a. Per il protocollo Server, scegli HTTPS.
b. Per Porta server, inserisci **443**.
c. Per Certificato, scegli il file del certificato per la connessione all'`s3apiendpoint`.

10. Seleziona Richiede credenziali e inserisci la chiave di accesso e la chiave segreta per accedere al bucket di storage compatibile con Amazon S3 sul tuo dispositivo o cluster Snowball Edge.
11. Scegli Next (Successivo).

Configurazione della località di destinazione per il trasferimento

La località di destinazione del trasferimento deve trovarsi nella stessa Regione AWS località in Account AWS cui è stato creato l'agente.

Prima di iniziare: assicurati di aver configurato la posizione di origine per il trasferimento.

Per configurare la posizione di destinazione del trasferimento utilizzando la DataSync console

1. Nella pagina Configura la posizione di destinazione, scegli Crea una nuova posizione o Scegli una posizione esistente per la risorsa AWS di archiviazione in cui stai trasferendo gli oggetti.

   Se stai creando una nuova posizione, consulta uno dei seguenti argomenti:

   - Amazon S3
   - Amazon EFS
   - FSx per Windows File Server
   - FSx per Lustre
   - FSx per OpenZFS
   - FSx per ONTAP
2. Quando hai finito di configurare la posizione di destinazione, scegli Avanti.

Configurazione delle impostazioni di trasferimento

Con DataSync, puoi specificare una pianificazione di trasferimento, personalizzare la modalità di verifica dell'integrità dei dati e specificare se desideri trasferire solo un sottoinsieme di oggetti, tra le altre opzioni.

Prima di iniziare: assicurati di aver configurato la località di destinazione per il trasferimento.

Per configurare le impostazioni di trasferimento utilizzando la DataSync console

1. Nella pagina Configura impostazioni, modifica le impostazioni di trasferimento o utilizza le impostazioni predefinite.

   Per ulteriori informazioni su queste impostazioni, consultare Scelta dei trasferimenti AWS DataSync.
2. Scegli Next (Successivo).
3. Controlla i dettagli del trasferimento, quindi scegli Crea attività.

Avvio del trasferimento

Dopo aver creato l'attività di trasferimento, sei pronto per iniziare a spostare i dati. Per istruzioni su come avviare un'attività utilizzando la DataSync console oppure AWS CLI, consulta Avvio dell'attività.

Limitazioni

- Se il sistema di storage di origine utilizza il protocollo NFS (ad esempio Amazon EFS), non è DataSync possibile trasferire file con collegamenti fisici a un dispositivo Snowball Edge.
- DataSync non può trasferire oggetti di lunghezza superiore a 1.024 byte da un dispositivo Snowball Edge a un bucket S3. Per ulteriori informazioni, consulta la Amazon S3 User Guide.

Creazione di un'attività per il trasferimento dei dati

Un'attività descrive dove e come vengono AWS DataSync trasferiti i dati. Un'attività è composta da quanto segue:

- Ubicazione di origine: il sistema o il servizio di storage da cui vengono DataSync trasferiti i dati.
- Ubicazione di destinazione: il sistema o il servizio di storage a cui vengono DataSync trasferiti i dati.
- Opzioni relative alle attività: impostazioni come i file da trasferire, il modo in cui i dati vengono verificati, quando viene eseguita l'attività e altro ancora.
- Esecuzioni di attività: quando si esegue un'attività, si parla di esecuzione di attività.

Creazione dell'attività

Quando si crea un' DataSync attività, si specificano le posizioni di origine e di destinazione. Puoi anche personalizzare l'attività scegliendo quali file trasferire, come vengono gestiti i metadati, impostando una pianificazione e altro ancora.

Prima di creare l'attività, assicurati di comprendere come funzionano DataSync i trasferimenti e di rivedere le quote delle attività.

> **Important**
>
> Se hai intenzione di trasferire dati da o verso una sede Amazon S3, consulta in che modo DataSync possono influire sui costi delle richieste S3 e sulla pagina dei DataSync prezzi prima di iniziare.

Utilizzo della console DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Assicurati di trovarti in uno dei Regioni AWS luoghi in cui intendi trasferire i dati.
3. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
4. Nella pagina Configura la posizione di origine, crea o scegli una posizione di origine, quindi scegli Avanti.
5. Nella pagina Configura la posizione di destinazione, crea o scegli una posizione di destinazione, quindi scegli Avanti.
6. (Consigliato) Nella pagina Configura impostazioni, assegna all'attività un nome facile da ricordare.
7. Nella pagina Configura impostazioni, scegli le opzioni relative all'attività o utilizza le impostazioni predefinite.

   Potrebbero interessarti alcune delle seguenti opzioni:

   - Specificate la modalità di attività che desiderate utilizzare.
   - Specificate quali dati trasferire utilizzando un manifesto o dei filtri.
   - Configura come gestire i metadati dei file e verificare l'integrità dei dati.

- Monitora il trasferimento con report sulle attività o Amazon CloudWatch. Ti consigliamo di impostare un qualche tipo di monitoraggio per la tua attività.

Al termine, selezionare Next (Successivo).

8. Controlla la configurazione dell'attività, quindi scegli Crea attività.

Sei pronto per iniziare la tua attività.

Usando il AWS CLI

Dopo aver creato le posizioni di DataSync origine e di destinazione, puoi creare l'attività.

1. Nelle AWS CLI impostazioni, assicurati di utilizzare uno dei Regioni AWS luoghi in cui intendi trasferire i dati.
2. Copia il seguente `create-task` comando:

```
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. Per`--source-location-arn`, specifica l'Amazon Resource Name (ARN) della tua posizione di origine.
4. Per`--destination-location-arn`, specifica l'ARN della località di destinazione.

   Se effettui trasferimenti tra Regioni AWS i nostri account, assicurati che l'ARN includa l'altra regione o l'ID dell'account.
5. (Consigliato) Per`--name`, specifica un nome facile da ricordare per l'attività.
6. Specificate altre opzioni di attività in base alle esigenze. Potrebbero interessarti alcune delle seguenti opzioni:

   - Specificate quali dati trasferire utilizzando un manifesto o dei filtri.
   - Configura come gestire i metadati dei file e verificare l'integrità dei dati.
   - Monitora il trasferimento con report sulle attività o Amazon CloudWatch. Ti consigliamo di impostare un qualche tipo di monitoraggio per la tua attività.

Per ulteriori opzioni, consulta create-task. Ecco un `create-task` comando di esempio che specifica diverse opzioni:

```
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" \
  --options
 VerifyMode=NONE,OverwriteMode=NEVER,Atime=BEST_EFFORT,Mtime=PRESERVE,Uid=INT_VALUE,Gid=INT
```

7. Esegui il comando `create-task`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN dell'attività creata. Per esempio:

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/task-08de6e6697796f026"
}
```

Sei pronto per iniziare la tua attività.

Stati delle attività

Quando crei un' DataSync attività, puoi controllarne lo stato per vedere se è pronta per l'esecuzione.

Stato della console	Stato dell'API	Descrizione
Disponibilità	`AVAILABLE`	L'attività è pronta per iniziare il trasferimento dei dati.
In esecuzione	`RUNNING`	È in corso l'esecuzione di un'operazione. Per ulteriori informazioni, consulta Stati di esecuzione delle attività.

Stato della console	Stato dell'API	Descrizione
Non disponibile	`UNAVAILABLE`	Un DataSync agente utilizzato dall'operazione è offline. Per ulteriori informazioni, consulta Cosa devo fare se il mio agente è offline?
Accodati	`QUEUED`	È in corso l'esecuzione di un'altra operazione che utilizza lo stesso DataSync agente. Per ulteriori informazioni, consulta Sapere quando l'attività è in coda.

Partizionamento di set di dati di grandi dimensioni con più attività

Se stai trasferendo un set di dati di grandi dimensioni, ad esempio la migrazione di milioni di file o oggetti, ti consigliamo di partizionare il set di dati con più attività. DataSync Il partizionamento dei dati di origine tra più attività (e possibilmente agenti, a seconda delle ubicazioni) aiuta a ridurre il tempo necessario per preparare e trasferire i dati. DataSync

Considerate alcuni dei modi in cui potete partizionare un set di dati di grandi dimensioni tra diverse attività: DataSync

- Crea attività che trasferiscono cartelle separate. Ad esempio, è possibile creare due attività destinate`/FolderB`, `/FolderA` rispettivamente, all'unità di archiviazione di origine.
- Crea attività che trasferiscono sottoinsiemi di file, oggetti e cartelle utilizzando un manifesto o filtri.

Tieni presente che questo approccio può aumentare I/O le operazioni sullo storage e influire sulla larghezza di banda della rete. Per ulteriori informazioni, consulta il blog su Come accelerare i trasferimenti di dati con architetture DataSync scalabili orizzontalmente.

Segmentazione dei dati trasferiti con più attività

Se trasferisci diversi set di dati verso la stessa destinazione, puoi creare più attività per segmentare i dati trasferiti.

Ad esempio, se stai trasferendo nello stesso bucket S3 denominato`MyBucket`, puoi creare prefissi diversi nel bucket che corrispondono a ciascuna attività. Questo approccio impedisce che i nomi dei file entrino in conflitto con i set di dati e consente di impostare autorizzazioni diverse per ogni prefisso. Ecco come puoi configurarlo:

1. Crea tre prefissi nella destinazione `MyBucket` denominata `task1` `etask2`: `task3`
   - `s3://MyBucket/task1`
   - `s3://MyBucket/task2`
   - `s3://MyBucket/task3`
2. Crea tre DataSync attività denominate `task1task2`, e `task3` trasferiscile al prefisso corrispondente in. `MyBucket`

Scelta di una modalità di operazione per il trasferimento dei dati

L' AWS DataSync attività può essere eseguita in una delle seguenti modalità:

- Modalità avanzata: trasferisci un numero virtualmente illimitato di oggetti con prestazioni superiori rispetto alla modalità Basic. Le attività in modalità avanzata ottimizzano il processo di trasferimento dei dati elencando, preparando, trasferendo e verificando i dati in parallelo. La modalità avanzata è attualmente disponibile per i trasferimenti tra sedi Amazon S3, i trasferimenti tra Azure Blob e Amazon S3 senza un agente e i trasferimenti tra altri cloud e Amazon S3 senza agente.
- Modalità base: trasferimento di file o oggetti tra AWS lo storage e tutte le altre posizioni supportate. DataSync Le attività in modalità base sono soggette a quote sul numero di file, oggetti e directory in un set di dati. La modalità base prepara, trasferisce e verifica i dati in modo sequenziale, rendendola più lenta della modalità avanzata per la maggior parte dei carichi di lavoro.

Comprensione delle differenze tra le modalità attività

Le seguenti informazioni possono aiutarti a determinare la modalità di attività da utilizzare.

Funzionalità	Comportamento della modalità migliorato	Comportamento in modalità base
Prestazioni	DataSync elenca, prepara, trasferisce e verifica i dati in parallelo. Fornisce prestazioni superiori rispetto alla modalità Basic per la maggior parte dei carichi di lavoro (come	DataSync prepara, trasferisce e verifica i dati in sequenza. Le prestazioni sono più lente della modalità Enhanced per la maggior parte dei carichi di lavoro

Funzionalità	Comportamento della modalità migliorato	Comportamento in modalità base
	il trasferimento di oggetti di grandi dimensioni)	
Numero di elementi in un set di dati che è DataSync possibile utilizzare per esecuzione di attività	Numero virtualmente illimitato di oggetti	Si applicano le quote
Contatori e metriche per il trasferimento dei dati	Più contatori e metriche rispetto alla modalità Basic, come il numero di oggetti DataSync trovati nella posizione di origine e quanti oggetti vengono preparati durante l'esecuzione di ogni attività	Meno contatori e metriche rispetto alla modalità Avanzata
Registrazione di log	Registri strutturati (formato JSON)	Registri non strutturati
Posizioni supportate	Attualmente per trasferimenti tra sedi Amazon S3, trasferim enti tra Azure Blob e Amazon S3 senza agente e trasferim enti tra altri cloud e Amazon S3 senza agente.	Per i trasferimenti tra tutte le sedi che supportano DataSync
Opzioni di verifica dei dati	DataSync verifica solo i dati trasferiti	DataSync verifica tutti i dati per impostazione predefinita
Limiti di larghezza di banda	Non applicabile	Supportato
Costo	Per ulteriori informazioni, consulta la pagina dei DataSync prezzi	Per ulteriori informazioni, consulta la pagina DataSync dei prezzi

Funzionalità	Comportamento della modalità migliorato	Comportamento in modalità base
Gestione degli errori per i tag degli oggetti non supportati	Per i trasferimenti di archiviazione cloud da o verso posizioni che non supportano il tagging degli oggetti, l'esecuzione dell'attività avrà esito negativo immediatamente se l'`ObjectTags` opzione non è specificata o è impostata su. `PRESERVE`	Per i trasferimenti di archiviazione cloud da o verso posizioni che non supportano il tagging degli oggetti, l'esecuzione dell'attività verrà eseguita normalmente, ma segnalerà gli errori per oggetto per gli oggetti con tag se l'opzione non è specificata o è impostata su. `ObjectTags` `PRESERVE`

Scelta di una modalità di attività

Puoi scegliere la modalità Enhanced solo per i trasferimenti tra sedi Amazon S3, i trasferimenti tra Azure Blob e Amazon S3 senza un agente e i trasferimenti tra altri cloud e Amazon S3 senza agente. Altrimenti, devi usare la modalità Basic. Ad esempio, un trasferimento da una posizione NFS locale a una posizione S3 richiede la modalità Basic.

Le opzioni e le prestazioni delle attività potrebbero variare a seconda della modalità di attività scelta. Una volta creata l'attività, non è possibile modificarne la modalità.

Autorizzazioni richieste

Per creare un'attività in modalità avanzata, il ruolo IAM DataSync con cui stai utilizzando deve disporre dell'`iam:CreateServiceLinkedRole`autorizzazione.

Per le autorizzazioni DataSync utente, valuta la possibilità di utilizzare AWSDataSyncFullAccess. Si tratta di una politica AWS gestita che fornisce all'utente l'accesso completo DataSync e un accesso minimo alle sue dipendenze.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.

2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per la modalità Attività, scegli una delle seguenti opzioni:

   - Avanzata
   - Base

   Per ulteriori informazioni, consulta Comprensione delle differenze tra le modalità attività.
5. Mentre sei ancora nella pagina Configura impostazioni, scegli altre opzioni di attività o utilizza le impostazioni predefinite.

   Potrebbero interessarti alcune delle seguenti opzioni:

   - Specificate quali dati trasferire utilizzando un manifesto o dei filtri.
   - Configura come gestire i metadati dei file e verificare l'integrità dei dati.
   - Monitora il trasferimento con report sulle attività o Amazon CloudWatch Logs.

   Al termine, selezionare Next (Successivo).
6. Controlla la configurazione delle attività, quindi scegli Crea attività.

Usando il AWS CLI

1. Nelle AWS CLI impostazioni, assicurati di utilizzare uno dei siti Regioni AWS in cui intendi trasferire i dati.
2. Copia il seguente `create-task` comando:

```
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. Per `--source-location-arn`, specifica l'Amazon Resource Name (ARN) della tua posizione di origine.
4. Per `--destination-location-arn`, specifica l'ARN della località di destinazione.

   Se effettui trasferimenti tra Regioni AWS i nostri account, assicurati che l'ARN includa l'altra regione o l'ID dell'account.
5. Per `--task-mode`, specifica `ENHANCED` o. `BASIC`

   Per ulteriori informazioni, consulta Comprensione delle differenze tra le modalità attività.
6. Specificate altre opzioni di attività in base alle esigenze. Potrebbero interessarti alcune delle seguenti opzioni:

   - Specificate quali dati trasferire utilizzando un manifesto o dei filtri.
   - Configura come gestire i metadati dei file e verificare l'integrità dei dati.
   - Monitora il trasferimento con report sulle attività o Amazon CloudWatch Logs.

   Per altre opzioni, consulta create-task. Ecco un `create-task` comando di esempio che specifica la modalità avanzata e diverse altre opzioni:

   ```
   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. Esegui il comando `create-task`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN dell'attività creata. Per esempio:

   ```
   {
       "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
   task-08de6e6697796f026"
   }
   ```

Utilizzo dell'API DataSync

È possibile specificare la modalità di DataSync operazione configurando il `TaskMode` parametro nell'CreateTaskoperazione.

Scelta dei trasferimenti AWS DataSync

AWS DataSync ti consente di scegliere cosa trasferire e come gestire i dati. Alcune opzioni includono:

- Trasferimento di un elenco esatto di file o oggetti utilizzando un manifesto.
- Inclusione o esclusione di determinati tipi di dati nel trasferimento utilizzando un filtro.
- Per i trasferimenti ricorrenti, sposta solo i dati modificati dall'ultimo trasferimento
- Sovrascrivere i dati nella posizione di destinazione in modo che corrispondano a quelli presenti nella posizione di origine.
- Scelta dei metadati del file o dell'oggetto da conservare tra le posizioni di archiviazione.

Argomenti

- Trasferimento di file o oggetti specifici utilizzando un manifesto
- Trasferimento di file, oggetti e cartelle specifici tramite filtri
- Comprendere come DataSync gestisce i metadati di file e oggetti
- Collegamenti e directory copiati da AWS DataSync
- Configurazione della modalità di gestione di file, oggetti e metadati

Trasferimento di file o oggetti specifici utilizzando un manifesto

Un manifesto è un elenco di file o oggetti che si AWS DataSync desidera trasferire. Ad esempio, invece di dover trasferire tutto in un bucket S3 con potenzialmente milioni di oggetti, DataSync trasferisce solo gli oggetti che elenchi nel tuo manifest.

I manifesti sono simili ai filtri ma consentono di identificare esattamente quali file o oggetti trasferire anziché i dati che corrispondono a uno schema di filtro.

Creazione del manifesto

Un manifesto è un file in formato CSV (valori separati da virgole) che elenca i file o gli oggetti che desideri trasferire nella posizione di origine. DataSync Se la tua fonte è un bucket S3, puoi anche includere la versione di un oggetto da trasferire.

Argomenti

- Linee guida
- Manifesti di esempio

Linee guida

Utilizza queste linee guida per aiutarti a creare un manifesto con cui funzionare. DataSync

Do

- Specificate il percorso completo di ogni file o oggetto che desiderate trasferire.

  Non è possibile specificare solo una directory o una cartella con l'intenzione di trasferirne tutto il contenuto. In queste situazioni, prendi in considerazione l'utilizzo di un filtro di inclusione anziché di un manifesto.
- Assicuratevi che il percorso di ogni file o oggetto sia relativo al percorso di montaggio, alla cartella, alla directory o al prefisso che avete specificato durante la configurazione della posizione di DataSync origine.

  Ad esempio, supponiamo che tu configuri una posizione S3 con un prefisso denominato. `photos` Tale prefisso include un oggetto `my-picture.png` che desideri trasferire. Nel manifesto, dovete quindi solo specificare l'oggetto (`my-picture.png`) anziché il prefisso e l'oggetto (`photos/my-picture.png`).
- Per specificare la versione dell'oggetto Amazon S3 IDs, separa il percorso e l'ID della versione dell'oggetto utilizzando una virgola.

  L'esempio seguente mostra una voce del manifesto con due campi. Il primo campo include un oggetto denominato`picture1.png`. Il secondo campo è separato da una virgola e include un ID di versione di`111111`:

  ```
  picture1.png,111111
  ```
- Usa le virgolette nelle seguenti situazioni:

- Quando un percorso contiene caratteri speciali (virgole, virgolette e terminazioni di riga):

  `"filename,with,commas.txt"`

- Quando un percorso si estende su più righe:

  ```
  "this
  is
  a
  filename.txt"
  ```

- Quando un percorso include virgolette:

  `filename""with""quotes.txt`

  Questo rappresenta un percorso denominato`filename"with"quotes.txt`.

  Queste regole di citazione si applicano anche ai campi ID di versione. In generale, se un campo manifesto contiene una virgoletta, è necessario evitarla inserendo un'altra citazione.

- Separate ogni voce di file o oggetto con una nuova riga.

  È possibile separare le righe utilizzando interruzioni di riga in stile Linux (line feed o carriage return) o Windows (carriage return seguito da line feed).

- Salva il tuo manifesto (ad esempio, `my-manifest.csv` o`my-manifest.txt`).
- Carica il manifesto in un bucket S3 a cui DataSync puoi accedere.

  Questo bucket non deve necessariamente trovarsi nello stesso account Regione AWS o nello stesso account in cui stai utilizzando. DataSync

Don't

- Specificate solo una directory o una cartella con l'intenzione di trasferirne tutto il contenuto.

  Un manifesto può includere solo i percorsi completi dei file o degli oggetti che si desidera trasferire. Se configurate la posizione di origine per utilizzare un percorso di montaggio, una cartella, una directory o un prefisso specifici, non è necessario includerlo nel manifesto.

- Specificate un percorso del file o dell'oggetto che superi i 4.096 caratteri.
- Specificare un percorso del file, un percorso dell'oggetto o un ID di versione dell'oggetto Amazon S3 che superi i 1.024 byte.

- Specificate i percorsi duplicati di file o oggetti.
- Includi un ID di versione dell'oggetto se la posizione di origine non è un bucket S3.
- Includi più di due campi in una voce del manifesto.

  Una voce può includere solo un percorso di file o oggetto e (se applicabile) un ID di versione dell'oggetto Amazon S3.
- Includi caratteri non conformi alla codifica UTF-8.
- Includi spazi non intenzionali nei campi di immissione al di fuori delle virgolette.

Manifesti di esempio

Usa questi esempi per aiutarti a creare un manifesto che funzioni con DataSync.

Manifesto con percorsi completi di file o oggetti

L'esempio seguente mostra un manifesto con i percorsi completi dei file o degli oggetti da trasferire.

```
photos/picture1.png
photos/picture2.png
photos/picture3.png
```

Manifest con solo chiavi di oggetto

L'esempio seguente mostra un manifesto con oggetti da trasferire da una posizione di origine di Amazon S3. Poiché la posizione è configurata con il prefisso`photos`, vengono specificate solo le chiavi dell'oggetto.

```
picture1.png
picture2.png
picture3.png
```

Manifesto con i percorsi e la versione degli oggetti IDs

Le prime due voci del seguente esempio di manifesto includono versioni specifiche di oggetti Amazon S3 da trasferire.

```
photos/picture1.png,111111
photos/picture2.png,121212
```

```
photos/picture3.png
```

Manifesto con caratteri UTF-8

L'esempio seguente mostra un manifesto con file che includono caratteri UTF-8.

```
documents/résumé1.pdf
documents/résumé2.pdf
documents/résumé3.pdf
```

Fornire DataSync l'accesso al manifesto

È necessario un ruolo AWS Identity and Access Management (IAM) che dia DataSync accesso al manifesto nel relativo bucket S3. Questo ruolo deve includere le seguenti autorizzazioni:

- `s3:GetObject`
- `s3:GetObjectVersion`

Puoi generare questo ruolo automaticamente nella DataSync console o crearlo tu stesso.

> **Note**
>
> Se il tuo manifesto si trova in un altro Account AWS, devi creare questo ruolo manualmente.

Creazione automatica del ruolo IAM

Quando crei o avvii un'attività di trasferimento nella console, DataSync puoi creare per te un ruolo IAM con le autorizzazioni `s3:GetObject` e `s3:GetObjectVersion` le autorizzazioni necessarie per accedere al tuo manifest.

Autorizzazioni necessarie per creare automaticamente il ruolo

Per creare automaticamente il ruolo, assicurati che il ruolo che stai utilizzando per accedere alla DataSync console disponga delle seguenti autorizzazioni:

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:AttachRolePolicy`

Creazione del ruolo IAM (stesso account)

Puoi creare manualmente il ruolo IAM che DataSync deve accedere al tuo manifest. Le seguenti istruzioni presuppongono che tu sia nello stesso posto in Account AWS cui lo usi DataSync e che si trovi il bucket S3 del tuo manifest.

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli, quindi scegli Crea ruolo.
3. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli Servizio AWS.
4. Per Caso d'uso, scegli DataSyncnell'elenco a discesa e seleziona DataSync. Scegli Next (Successivo).
5. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo). Dai un nome al tuo ruolo e scegli Crea ruolo.
6. Nella pagina Ruoli, cerca il ruolo che hai appena creato e scegline il nome.
7. Nella pagina dei dettagli del ruolo, scegli la scheda Autorizzazioni. Scegli Aggiungi autorizzazioni, quindi Crea politica in linea.
8. Scegli la scheda JSON e incolla la seguente politica di esempio nell'editor delle politiche:

   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. Nella policy di esempio che hai appena incollato, sostituisci i seguenti valori con i tuoi:

   a. Sostituiscilo *amzn-s3-demo-bucket* con il nome del bucket S3 che ospita il tuo manifest.

   b. *my-manifest.csv*Sostituiscilo con il nome del file del tuo manifest.

10. Scegli Next (Successivo). Dai un nome alla tua politica e scegli Crea politica.
11. (Consigliato) Per evitare il problema del sostituto confuso tra diversi servizi, procedi come segue:

    a. Nella pagina dei dettagli del ruolo, scegli la scheda Relazioni di fiducia. Seleziona Modifica policy di attendibilità.

    b. Aggiorna la politica di fiducia utilizzando l'esempio seguente, che include le chiavi del contesto `aws:SourceArn` e della condizione `aws:SourceAccount` globale:

       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:*"
            }
        }
      }
  ]
}
```

       - Sostituisci ogni istanza *account-id* con l' Account AWS ID in cui stai utilizzando DataSync.
       - Sostituisci *region* Regione AWS con quello che stai utilizzando DataSync.

    c. Scegli Aggiorna policy.

Hai creato un ruolo IAM che consente di accedere DataSync al tuo manifest. Specificate questo ruolo al momento della creazione o dell'avvio dell'attività.

Creazione del ruolo IAM (account diverso)

Se il tuo manifest si trova in un bucket S3 che appartiene a un altro Account AWS, devi creare manualmente il ruolo IAM da DataSync utilizzare per accedere al manifest. Quindi, nel luogo in Account AWS cui si trova il manifesto, devi includere il ruolo nella policy del bucket S3.

Creazione del ruolo

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli, quindi scegli Crea ruolo.
3. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli Servizio AWS.
4. Per Caso d'uso, scegli DataSyncnell'elenco a discesa e seleziona DataSync. Scegli Next (Successivo).
5. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo). Dai un nome al tuo ruolo e scegli Crea ruolo.
6. Nella pagina Ruoli, cerca il ruolo che hai appena creato e scegline il nome.
7. Nella pagina dei dettagli del ruolo, scegli la scheda Autorizzazioni. Scegli Aggiungi autorizzazioni, quindi Crea politica in linea.
8. Scegli la scheda JSON e incolla la seguente politica di esempio nell'editor delle politiche:

   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. Nella policy di esempio che hai appena incollato, sostituisci i seguenti valori con i tuoi:

   a. Sostituiscilo *amzn-s3-demo-bucket* con il nome del bucket S3 che ospita il tuo manifest.

b. *my-manifest.csv*Sostituiscilo con il nome del file del tuo manifest.

10. Scegli Next (Successivo). Dai un nome alla tua politica e scegli Crea politica.
11. (Consigliato) Per evitare il problema del sostituto confuso tra diversi servizi, procedi come segue:

    a. Nella pagina dei dettagli del ruolo, scegli la scheda Relazioni di fiducia. Seleziona Modifica policy di attendibilità.

    b. Aggiorna la politica di fiducia utilizzando l'esempio seguente, che include le chiavi del contesto `aws:SourceArn` e della condizione `aws:SourceAccount` globale:

    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:*"
            }
        }
     }
  ]
}
```

    - Sostituisci ogni istanza di *account-id* con l' Account AWS ID in cui stai utilizzando DataSync.
    - Sostituisci *region* Regione AWS con quello che stai utilizzando DataSync.

    c. Scegli Aggiorna policy.

Hai creato il ruolo IAM che puoi includere nella tua policy sui bucket S3.

Aggiornamento della policy sui bucket S3 con il ruolo

Dopo aver creato il ruolo IAM, devi aggiungerlo alla policy del bucket S3 nell'altro Account AWS posto in cui si trova il tuo manifest.

1. Quindi AWS Management Console, passa all'account con il bucket S3 del tuo manifesto.
2. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
3. Nella pagina dei dettagli del bucket, scegli la scheda Autorizzazioni.
4. In Bucket policy, scegli Modifica e procedi come segue per modificare la tua policy sui bucket S3:

   a. Aggiorna il contenuto dell'editor per includere le seguenti dichiarazioni politiche:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "DataSyncAccessManifestBucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:role/datasync-role"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

   b. Sostituiscilo *account-id* con l' Account AWS ID dell'account DataSync con cui stai utilizzando.

   c. Sostituiscilo *datasync-role* con il ruolo IAM che hai appena creato che consente di accedere DataSync al tuo manifest.

   d. Sostituiscilo *amzn-s3-demo-bucket* con il nome del bucket S3 che ospita il tuo manifest nell'altro. Account AWS

5. Scegli Save changes (Salva modifiche).

Hai creato un ruolo IAM che consente di accedere DataSync al tuo manifest nell'altro account. Specificate questo ruolo al momento della creazione o dell'avvio dell'attività.

Specificare il manifesto durante la creazione di un'attività

È possibile specificare il manifesto che si desidera DataSync utilizzare durante la creazione di un'attività.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Attività, quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per i contenuti da scansionare, scegli File, oggetti e cartelle specifici, quindi seleziona Utilizzo di un manifesto.
5. Per l'URI S3, scegli il tuo manifest ospitato su un bucket S3.

   In alternativa, puoi inserire l'URI (ad esempio,). `s3://bucket/prefix/my-manifest.csv`
6. Per la versione dell'oggetto, scegliete la versione del manifesto che desiderate DataSync utilizzare.

   Per impostazione predefinita, DataSync utilizza la versione più recente dell'oggetto.
7. Per il ruolo di accesso Manifest, effettuate una delle seguenti operazioni:

   - Scegli Autogenerate for per DataSync creare automaticamente un ruolo IAM con le autorizzazioni necessarie per accedere al tuo manifest nel suo bucket S3.
   - Scegli un ruolo IAM esistente in grado di accedere al tuo manifest.

   Per ulteriori informazioni, consulta Fornire DataSync l'accesso al manifesto.
8. Configura tutte le altre impostazioni di attività di cui hai bisogno, quindi scegli Avanti.
9. Scegli Create task (Crea attività).

Utilizzando il AWS CLI

1. Copia il seguente `create-task` comando:

```
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. Per il `--source-location-arn` parametro, specifica l'Amazon Resource Name (ARN) della posizione da cui stai trasferendo i dati.
3. Per il `--destination-location-arn` parametro, specifica l'ARN della posizione in cui stai trasferendo i dati.
4. Per il `--manifest-config` parametro, effettuate le seguenti operazioni:

   - `ManifestObjectPath`— Specificate la chiave dell'oggetto S3 del vostro manifest.
   - `BucketAccessRoleArn`— Specificate il ruolo IAM che consente di accedere DataSync al vostro manifest nel suo bucket S3.

     Per ulteriori informazioni, consulta Fornire DataSync l'accesso al manifesto.

   - `S3BucketArn`— Specificate l'ARN del bucket S3 che ospita il vostro manifest.
   - `ManifestObjectVersionId`— Specificate la versione del manifesto che desiderate DataSync utilizzare.

     Per impostazione predefinita, DataSync utilizza la versione più recente dell'oggetto.
5. Esegui il `create-task` comando per creare l'attività.

Quando sei pronto, puoi iniziare l'operazione di trasferimento.

Specificare il manifesto all'avvio di un'attività

È possibile specificare il manifesto che si desidera DataSync utilizzare durante l'esecuzione di un'attività.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Attività, quindi scegli l'attività che desideri avviare.
3. Nella pagina di panoramica delle attività, scegli Avvia, quindi scegli Inizia con opzioni di sovrascrittura.
4. Per i contenuti da scansionare, scegli File, oggetti e cartelle specifici, quindi seleziona Utilizzo di un manifesto.
5. Per l'URI S3, scegli il tuo manifest ospitato su un bucket S3.

   In alternativa, puoi inserire l'URI (ad esempio,). `s3://bucket/prefix/my-manifest.csv`
6. Per la versione dell'oggetto, scegliete la versione del manifesto che desiderate DataSync utilizzare.

   Per impostazione predefinita, DataSync utilizza la versione più recente dell'oggetto.
7. Per il ruolo di accesso Manifest, effettuate una delle seguenti operazioni:

   - Scegli Autogenerate for per DataSync creare automaticamente un ruolo IAM per accedere al tuo manifest nel suo bucket S3.
   - Scegli un ruolo IAM esistente che possa accedere al tuo manifest.

   Per ulteriori informazioni, consulta Fornire DataSync l'accesso al manifesto.
8. Scegli Inizia per iniziare il trasferimento.

Usando il AWS CLI

1. Copia il seguente `start-task-execution` comando:

```
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. Per il `--task-arn` parametro, specifica l'Amazon Resource Name (ARN) dell'attività che stai avviando.
3. Per il `--manifest-config` parametro, procedi come segue:
   - `ManifestObjectPath`— Specificate la chiave dell'oggetto S3 del vostro manifest.
   - `BucketAccessRoleArn`— Specificate il ruolo IAM che consente di accedere DataSync al vostro manifest nel suo bucket S3.

     Per ulteriori informazioni, consulta Fornire DataSync l'accesso al manifesto.

   - `S3BucketArn`— Specificate l'ARN del bucket S3 che ospita il vostro manifest.
   - `ManifestObjectVersionId`— Specificate la versione del manifesto che desiderate DataSync utilizzare.

     Per impostazione predefinita, DataSync utilizza la versione più recente dell'oggetto.
4. Esegui il `start-task-execution` comando per iniziare il trasferimento.

Limitazioni

- Non puoi usare un manifesto insieme ai filtri.
- Non è possibile specificare solo una directory o una cartella con l'intenzione di trasferirne tutto il contenuto. In queste situazioni, prendi in considerazione l'utilizzo di un filtro di inclusione anziché di un manifesto.
- Non è possibile utilizzare l'opzione Keep deleted files task (`PreserveDeletedFiles`nell'API) per mantenere file o oggetti nella destinazione che non si trovano nell'origine. DataSync trasferisce solo ciò che è elencato nel manifesto e non elimina nulla nella destinazione.

Risoluzione dei problemi

Se trasferisci oggetti con una versione specifica IDs da un bucket S3, potresti visualizzare un errore relativo a o. `HeadObject` `GetObjectTagging` Ad esempio, ecco un errore relativo a: `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
```

Se riscontri uno di questi errori, verifica che il ruolo IAM DataSync utilizzato per accedere alla posizione di origine di S3 disponga delle seguenti autorizzazioni:

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

Se devi aggiornare il tuo ruolo con queste autorizzazioni, consulta. Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3

Passaggi successivi

Se non l'hai già fatto, inizia la tua attività. Altrimenti, monitora l'attività della tua attività.

Trasferimento di file, oggetti e cartelle specifici tramite filtri

AWS DataSync consente di applicare filtri per includere o escludere dati dalla posizione di origine in un trasferimento. Ad esempio, se non desideri trasferire file temporanei che terminano con `.tmp`, puoi creare un filtro di esclusione in modo che questi file non raggiungano la posizione di destinazione.

È possibile utilizzare una combinazione di filtri di esclusione e inclusione nella stessa operazione di trasferimento. Se modifichi i filtri di un'attività, tali modifiche vengono applicate alla successiva esecuzione dell'attività.

Filtraggio di termini, definizioni e sintassi

Acquisisci familiarità con i concetti relativi al filtraggio: DataSync

Filtro

L'intera stringa che costituisce un particolare filtro (ad esempio, `*.tmp | *.temp` o). `/folderA|/folderB`

I filtri sono costituiti da motivi delimitati da una barra verticale (|). Non è necessario un delimitatore quando si aggiungono motivi nella DataSync console perché ogni motivo viene aggiunto separatamente.

> **Note**
>
> I filtri distinguono tra maiuscole e minuscole Ad esempio, il filtro `/folderA` non corrisponderà`/FolderA`.

Pattern

Un modello all'interno di un filtro. Ad esempio, `*.tmp` è un pattern che fa parte del `*.tmp | *.temp` filtro. Se il filtro ha più pattern, è possibile delimitare ogni pattern utilizzando una pipe (|).

Cartelle

- Tutti i filtri sono relativi al percorso della posizione di origine. Ad esempio, supponete di specificare `/my_source/` come percorso di origine quando create la posizione e l'attività di origine e di specificare il filtro di inclusione. `/transfer_this/` In questo caso, DataSync trasferisce solo la directory `/my_source/transfer_this/` e il relativo contenuto.
- Per specificare una cartella direttamente nella posizione di origine, includi una barra (/) davanti al nome della cartella. Nell'esempio precedente, il modello utilizza `/transfer_this`, non `transfer_this`.
- DataSync interpreta i seguenti modelli allo stesso modo e corrisponde sia alla cartella che al suo contenuto.

  `/dir`

  `/dir/`
- Quando trasferisci dati da o verso un bucket Amazon S3 DataSync, considera `/` il carattere nella chiave oggetto come l'equivalente di una cartella su un file system.

Caratteri speciali

Di seguito sono riportati i caratteri speciali per l'uso con i filtri.

Carattere speciale	Descrizione
* (carattere jolly)	Un carattere usato per la corrispondenza con zero o più caratteri. Ad esempio, `/movies_folder*` corrisponde a `/movies_folder` e `/movies_folder1`.
| (delimitatore pipe)	Un carattere utilizzato come delimitatore tra modelli. Consente di specificare più modelli, uno dei quali corrisponde al filtro. Ad esempio, `*.tmp|*.temp` corrisponde ai file che terminano con `tmp` o `temp`. **Note** Questo delimitatore non è necessario quando si aggiungono motivi sulla console perché si aggiunge ogni motivo su una riga separata.
\ (barra rovesciata)	Un carattere usato per sfuggire ai caratteri speciali (*, |,\) in un nome di file o oggetto. Una barra rovesciata doppia (\\) è obbligatoria quando una barra rovesciata fa parte di un nome file. Analogamente, \\\\ rappresenta due barre rovesciate consecutive in un nome file. Una barra rovesciata da una pipe (\ |) è obbligatoria quando una pipe fa parte di un nome file. Una barra rovesciata (\) seguita da qualsiasi altro carattere o alla fine di uno schema viene ignorata.

Filtri di esempio

I seguenti esempi mostrano i filtri più comuni con cui è possibile utilizzare DataSync.

> **Note**
>
> Esistono dei limiti al numero di caratteri che è possibile utilizzare in un filtro. Per ulteriori informazioni, consulta DataSync quote.

Esclusione di alcune cartelle dalla posizione di origine

In alcuni casi, potresti voler escludere le cartelle nella posizione di origine per non copiarle nella posizione di destinazione. Ad esempio, se hai work-in-progress cartelle temporanee, puoi usare qualcosa come il seguente filtro:

```
*/.temp
```

Per escludere cartelle con contenuti simili (come `/reports2021` e`/reports2022`)), puoi utilizzare un filtro di esclusione come il seguente:

```
/reports*
```

Per escludere cartelle a qualsiasi livello nella gerarchia dei file, puoi utilizzare un filtro di esclusione come il seguente.

```
*/folder-to-exclude-1|*/folder-to-exclude-2
```

Per escludere le cartelle al livello superiore della posizione di origine, puoi utilizzare un filtro di esclusione come il seguente.

```
/top-level-folder-to-exclude-1|/top-level-folder-to-exclude-2
```

Includi un sottoinsieme di cartelle nella posizione di origine

In alcuni casi, la posizione di origine potrebbe essere una condivisione di grandi dimensioni ed è necessario trasferire un sottoinsieme delle cartelle nella cartella principale. Per includere cartelle specifiche, avvia un'esecuzione dell'attività con un filtro di inclusione come il seguente.

```
/folder-to-transfer/*
```

Escludere tipi di file specifici

Per escludere alcuni tipi di file dal trasferimento, puoi creare un'esecuzione dell'attività con un filtro di esclusione come `*.temp`.

Trasferisci singoli file da te specificati

Per trasferire un elenco di singoli file, avviate l'esecuzione di un'attività con un filtro di inclusione come il seguente: "`/folder/subfolder/file1.txt`| `/folder/subfolder/file2.txt` |`/folder/subfolder/file2.txt`»

Creazione di filtri di inclusione

I filtri di inclusione definiscono i file, gli oggetti e le cartelle che si desidera DataSync trasferire. È possibile configurare i filtri di inclusione quando si crea, si modifica o si avvia un'attività.

DataSync esegue la scansione e trasferisce solo i file e le cartelle che corrispondono ai filtri di inclusione. Ad esempio, per includere un sottoinsieme delle cartelle di origine, è possibile specificare `/important_folder_1` |. `/important_folder_2`

> **Note**
>
> I filtri di inclusione supportano il carattere jolly (*) solo come carattere più a destra in uno schema. Ad esempio, `/documents*` | `/code*` è supportato, ma non `*.txt` lo è.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Attività, quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per i contenuti da scansionare, scegli File, oggetti e cartelle specifici, quindi seleziona Utilizzo dei filtri.
5. Per Include, inserisci il filtro (ad esempio, `/important_folders` per includere una directory importante), quindi scegli Aggiungi modello.
6. Aggiungi altri filtri di inclusione, se necessario.

Usando il AWS CLI

Quando si utilizza il AWS CLI, è necessario utilizzare le virgolette singole (`'`) attorno al filtro e un | (pipe) come delimitatore se si dispone di più di un filtro.

L'esempio seguente specifica due filtri di inclusione `/important_folder1` e `/important_folder2` quando si esegue il comando. `create-task`

```
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'
```

Creazione di filtri di esclusione

I filtri di esclusione definiscono i file, gli oggetti e le cartelle nella posizione di origine che non desideri DataSync trasferire. Puoi configurare questi filtri quando crei, modifichi o inizi un'attività.

Argomenti

- Dati esclusi per impostazione predefinita

Dati esclusi per impostazione predefinita

DataSync esclude automaticamente alcuni dati dal trasferimento:

- `.snapshot`— DataSync ignora qualsiasi percorso che termina con`.snapshot`, che in genere viene utilizzato per le point-in-time istantanee dei file o delle directory di un sistema di storage.
- `/.aws-datasync` `/.awssync` — DataSync crea queste cartelle nella posizione dell'utente per facilitare il trasferimento.
- `/.zfs`— Potresti vedere questa cartella con le sedi di Amazon FSx for OpenZFS.

Utilizzo della console DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Attività, quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per Escludi, inserisci il filtro (ad esempio, `*/temp` per escludere le cartelle temporanee), quindi scegli Aggiungi modello.
5. Aggiungi altri filtri di esclusione, se necessario.

6. Se necessario, aggiungi filtri di inclusione.

Usando il AWS CLI

Quando si utilizza il AWS CLI, è necessario utilizzare le virgolette singole (') attorno al filtro e un | (pipe) come delimitatore se si dispone di più di un filtro.

L'esempio seguente specifica due filtri di esclusione `*/temp` e `*/tmp` quando esegue il comando. `create-task`

```
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'
```

Comprendere come DataSync gestisce i metadati di file e oggetti

AWS DataSync può conservare i metadati del file o dell'oggetto durante un trasferimento di dati. Il modo in cui i metadati vengono copiati dipende dalle località di trasferimento e dal fatto che tali sedi utilizzino tipi di metadati simili.

Metadati a livello di sistema

In generale, DataSync non copia i metadati a livello di sistema. Ad esempio, durante il trasferimento da un file server SMB, le autorizzazioni configurate a livello di file system non vengono copiate nel sistema di storage di destinazione.

Esistono delle eccezioni. Durante il trasferimento tra Amazon S3 e altri sistemi di storage di oggetti DataSync , copia alcuni metadati di oggetti definiti dal sistema.

Metadati copiati nei trasferimenti Amazon S3

Le tabelle seguenti descrivono quali metadati DataSync possono essere copiati quando un trasferimento coinvolge una posizione Amazon S3.

Argomenti

- Per Amazon S3
- Tra Amazon S3 e altri sistemi di storage di oggetti

- Tra Amazon S3 e HDFS

Per Amazon S3

Quando si esegue la copia da una di queste posizioni	Verso questa posizione	DataSync può copiare
• NFS • Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS)	• Amazon S3	Di seguito sono riportati i metadati utente di Amazon S3: • Timestamp di modifica di file e cartelle • Timestamp di accesso a file e cartelle (DataSync è possibile farlo solo se possibile) • ID utente e ID gruppo • Autorizzazioni POSIX I metadati dei file archiviati nei metadati utente di Amazon S3 sono interoperabili con le condivisioni NFS sui gateway di file utilizzando. AWS Storage Gateway Un gateway di file consente l'accesso a bassa latenza dalle reti locali ai dati copiati su Amazon S3 da. DataSync Questi metadati sono interoperabili anche con for Lustre. FSx Quando DataSync copia gli oggetti che contengon o questi metadati su un server NFS, i metadati del file

Quando si esegue la copia da una di queste posizioni	Verso questa posizione	DataSync può copiare
		vengono ripristinati. Il ripristino dei metadati richiede la concessione di autorizzazioni elevate al server NFS. Per ulteriori informazioni, consulta Configurazione dei AWS DataSync trasferimenti con un file server NFS.

Tra Amazon S3 e altri sistemi di storage di oggetti

Quando si esegue la copia tra queste posizioni	DataSync può copiare

• Archiviazione di oggetti
• Amazon S3
	• Metadati di oggetti definiti dall'utente
	• Tag dell'oggetto
	• I seguenti metadati degli oggetti definiti dal sistema:
	  • Content-Disposition
	  • Content-Encoding
	  • Content-Language
	  • Content-Type
	
	Nota: DataSync copia i metadati a livello di sistema per tutti gli oggetti durante un trasferimento iniziale. Se configurate l'attività in modo da trasferire solo i dati che sono stati modificati, DataSync non copierà i metadati di sistema nei trasferimenti successivi, a meno che non siano stati modificati anche il contenuto di un oggetto o i metadati utente.

• Microsoft Azure Blob Storage • Amazon S3	

Quando si esegue la copia tra queste posizioni	DataSync può copiare
	DataSync non copia altri metadati degli oggetti, come le liste di controllo dell'accesso agli oggetti (ACLs), le versioni precedenti degli oggetti o la chiave Last-Modified.

Tra Amazon S3 e HDFS

Quando si esegue la copia tra queste posizioni	DataSync può copiare
• File system distribuito Hadoop (HDFS) • Amazon S3	Di seguito sono riportati i metadati utente di Amazon S3: • Timestamp di modifica di file e cartelle • Timestamp di accesso a file e cartelle (DataSync è possibile farlo solo se possibile) • ID utente e ID gruppo • Autorizzazioni POSIX HDFS utilizza stringhe per archiviare la proprietà di utenti e gruppi di file e cartelle, anziché identificatori numerici, come e. UIDs GIDs

Metadati copiati nei trasferimenti NFS

La tabella seguente descrive quali metadati DataSync possono essere copiati tra posizioni che utilizzano Network File System (NFS).

Quando si esegue la copia tra queste posizioni	DataSync può copiare
• NFS • Amazon EFS	• Timestamp di modifica di file e cartelle • Timestamp di accesso a file e cartelle (DataSync è possibile farlo solo se possibile)

Quando si esegue la copia tra queste posizioni	DataSync può copiare
• Amazon FSx per Lustre • Amazon FSx per OpenZFS • Amazon FSx per NetApp ONTAP (tramite NFS)	• ID utente (UID) e ID di gruppo (GID) • Autorizzazioni POSIX

Metadati copiati nei trasferimenti SMB

La tabella seguente descrive quali metadati DataSync possono essere copiati tra posizioni che utilizzano Server Message Block (SMB).

Quando si esegue la copia tra queste posizioni	DataSync può copiare
• SMB • File server Amazon FSx per Windows • FSx per ONTAP (utilizzando SMB)	• Timestamp dei file: tempo di accesso, tempo di modifica e tempo di creazione • Identificatore di sicurezza del proprietario del file (SID) • Attributi standard dei file: sola lettura (R), archivio (A), sistema (S), nascosto (H), compresso (C), non indicizzato il contenuto (I), crittografato (E), temporaneo (T), offline (O) e sparso (P) DataSync tenta di copiare gli attributi di archivio (A), compressi (C), non indicizzati dal contesto (I), sparsi (P) e temporanei (T) con il massimo impegno. Se questi attributi non vengono applicati alla destinazione, vengono ignorati durante la verifica dell'atti vità. • Elenchi di accesso discrezionali NTFS (DACLs), che determinano se concedere l'accesso a un oggetto. • Liste di controllo degli accessi al sistema NTFS (SACLs), utilizzate dagli amministr

Quando si esegue la copia tra queste posizioni	DataSync può copiare
	atori per registrare i tentativi di accesso a un oggetto protetto. Nota: non SACLs vengono copiati se si utilizza la versione 1.0 di SMB. La copia SACLs richiede DACLs la concessio ne di autorizzazioni specifiche all'utente Windows che DataSync utilizza SMB per accedere alla posizione dell'utente. Per ulteriori informazioni, consulta Creazione di una posizione per SMB, FSx per Windows File Server o FSx per ONTAP (a seconda del tipo di posizione nel trasferimento).

Metadati copiati in altri scenari di trasferimento

DataSync gestisce i metadati nei seguenti modi durante la copia tra questi sistemi di storage (la maggior parte dei quali ha strutture di metadati diverse).

Quando si esegue la copia da una di queste posizioni	Verso una di queste posizioni	DataSync può copiare
• SMB • FSx per Windows File Server • FSx per ONTAP (utilizzando SMB)	• Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS) • Amazon S3 • Archiviazione di oggetti • Azure Blob Storage • NFS	Metadati POSIX predefiniti per tutti i file e le cartelle sul file system di destinazione o per gli oggetti nel bucket S3 di destinazione. Questo approccio include l'utilizzo dei valori di ID utente POSIX e di ID gruppo predefiniti. I metadati basati su Windows (ad esempio) non vengono conservati. ACLs

Quando si esegue la copia da una di queste posizioni	Verso una di queste posizioni	DataSync può copiare
• Archiviazione di oggetti • Amazon S3 • Azure Blob Storage	• Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS)	Metadati POSIX predefiniti nei file e nelle cartelle di destinazione. Questo approccio include l'utilizzo dei valori di ID utente POSIX e di ID gruppo predefiniti.
• Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS)	• Azure Blob Storage	Quanto segue come metadati definiti dall'utente: • Timestamp di modifica di file e cartelle • Timestamp di accesso a file e cartelle (DataSync è possibile farlo solo se possibile) • ID utente e ID gruppo • Autorizzazioni POSIX

Quando si esegue la copia da una di queste posizioni	Verso una di queste posizioni	DataSync può copiare
• HDFS	• Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS)	• Timestamp di modifica di file e cartelle • Timestamp di accesso a file e cartelle (è DataSync possibile farlo solo con la massima diligenza) • Autorizzazioni POSIX HDFS archivia la proprietà di utenti e gruppi di file e cartelle come stringhe anziché come identificatori numerici (come e). UIDs GIDs I valori predefini ti per UIDs e GIDs vengono applicati al file system di destinazione. Per ulteriori informazioni, consulta Capire quando e come DataSync applicare i metadati POSIX predefiniti.
• Amazon S3 • Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per Windows File Server • FSx per ONTAP	• HDFS	Timestamp di file e cartelle dalla posizione di origine. Il proprietario del file o della cartella viene impostato in base all'utente HDFS o al principale Kerberos specifica to durante la creazione della posizione di trasferimento HDFS. La configurazione Groups Mapping sul cluster Hadoop determina il gruppo.

Quando si esegue la copia da una di queste posizioni	Verso una di queste posizioni	DataSync può copiare
• Amazon S3 • Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS) • Archiviazione di oggetti • NFS • HDFS	• SMB • FSx per Windows File Server • FSx per ONTAP (utilizzando SMB)	Timestamp di file e cartelle dalla posizione di origine. La proprietà viene impostata in base all'utente Windows specificato in DataSync per accedere alla condivisi one Amazon FSx o SMB. Le autorizzazioni vengono ereditate dalla directory principale.
• Azure Blob Storage	• FSx per Windows File Server • FSx per ONTAP (utilizzando SMB)	

Capire quando e come DataSync applicare i metadati POSIX predefiniti

DataSync applica i metadati POSIX predefiniti nelle seguenti situazioni:

- Quando le posizioni di origine e di destinazione del trasferimento non hanno strutture di metadati simili
- Quando mancano i metadati nella posizione di origine

La tabella seguente descrive come DataSync applicare i metadati POSIX predefiniti durante questi tipi di trasferimenti:

Origine	Destinazione	Autorizza zioni di file	Autorizza zioni per le cartelle	UID	GID
• Amazon S3 [1]	• Amazon EFS	0755	0755	65534	65534

Origine	Destinazione	Autorizzazioni di file	Autorizzazioni per le cartelle	UID	GID
• Archiviazione di oggetti 1 • Archiviazione BLOB di Microsoft Azure 1	• FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS) • NFS				
• SMB	• Amazon S3 • Archiviazione di oggetti • Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS) • NFS	0644	0755	65534	65534

Origine	Destinazione	Autorizzazioni di file	Autorizzazioni per le cartelle	UID	GID
• HDFS	• Amazon EFS • FSx per Lustre • FSx per OpenZFS • FSx per ONTAP (usando NFS) • NFS	0644	0755	65534	65534

[1] Nei casi in cui gli oggetti non dispongono di metadati precedentemente applicati da. DataSync

Collegamenti e directory copiati da AWS DataSync

AWS DataSync gestisce i link fisici, i link simbolici e le directory in modo diverso a seconda delle posizioni di archiviazione coinvolte nel trasferimento.

Collegamenti fissi

Ecco come DataSync gestisce gli hard link in alcuni scenari di trasferimento comuni:

- Durante il trasferimento tra un file server NFS, FSx per Lustre, per OpenZFS, FSx FSx per ONTAP (utilizzando NFS) e Amazon EFS, gli hard link vengono preservati.
- Durante il trasferimento su Amazon S3, ogni file sottostante a cui fa riferimento un collegamento fisico viene trasferito una sola volta. Durante i trasferimenti incrementali, vengono creati oggetti separati nel bucket S3. Se un collegamento fisico rimane invariato in Amazon S3, viene ripristinato correttamente quando viene trasferito su un file server NFS FSx , per Lustre, per OpenZFS FSx FSx , per ONTAP (usando NFS) o Amazon EFS.
- Durante il trasferimento suMicrosoft Azure Blob Storage, ogni file sottostante a cui fa riferimento un collegamento fisico viene trasferito una sola volta. Durante i trasferimenti incrementali, vengono creati oggetti separati nell'archivio BLOB se sono presenti nuovi riferimenti nell'origine. Durante

il trasferimento daAzure Blob Storage, DataSync trasferisce i collegamenti fisici come se fossero singoli file.

- Durante il trasferimento tra un file server SMB, FSx per Windows File Server e FSx per ONTAP (utilizzando SMB), gli hard link non sono supportati. Se vengono DataSync rilevati collegamenti fisici in queste situazioni, l'operazione di trasferimento viene completata con un errore. Per saperne di più, controlla i tuoi registri. CloudWatch
- Durante il trasferimento su HDFS, gli hard link non sono supportati. CloudWatch i registri mostrano che questi collegamenti sono stati ignorati.

Link simbolici

Ecco come DataSync gestisce i link simbolici in alcuni scenari di trasferimento comuni:

- Durante il trasferimento tra un file server NFS, FSx per Lustre, per OpenZFS, FSx FSx per ONTAP (utilizzando NFS) e Amazon EFS, i collegamenti simbolici vengono preservati.
- Durante il trasferimento su Amazon S3, il percorso di destinazione del collegamento viene archiviato nell'oggetto Amazon S3. Il collegamento viene ripristinato correttamente quando viene trasferito su un file server NFS, FSx per Lustre, FSx per OpenZFS, FSx per ONTAP o Amazon EFS.
- Durante il trasferimento a, i link simbolici non sono Azure Blob Storage supportati. CloudWatch i registri mostrano questi collegamenti come ignorati.
- Durante il trasferimento tra un file server SMB, FSx per Windows File Server e FSx per ONTAP (utilizzando SMB), i collegamenti simbolici non sono supportati. DataSync non trasferisce un collegamento simbolico di per sé, ma un file a cui fa riferimento il collegamento simbolico. Per riconoscere i file duplicati e deduplicarli con collegamenti simbolici, è necessario configurare la deduplicazione sul file system di destinazione.
- Durante il trasferimento su HDFS, i link simbolici non sono supportati. CloudWatch i registri mostrano che questi collegamenti sono stati ignorati.

Directory

In generale, DataSync conserva le directory durante il trasferimento tra sistemi di storage. Questo non è il caso nelle seguenti situazioni:

- Durante il trasferimento su Amazon S3, le directory sono rappresentate come oggetti vuoti con prefissi e terminano con una barra (). `/`

- Quando si esegue un trasferimento Azure Blob Storage senza uno spazio dei nomi gerarchico, le directory non esistono. Quella che sembra una directory è solo una parte del nome di un oggetto.

Configurazione della modalità di gestione di file, oggetti e metadati

È possibile configurare la modalità di AWS DataSync gestione dei file, degli oggetti e dei metadati associati durante il trasferimento tra posizioni.

Ad esempio, con i trasferimenti ricorrenti, potresti voler sovrascrivere i file nella destinazione modificando l'origine per mantenere sincronizzate le posizioni. È possibile copiare proprietà come le autorizzazioni POSIX per file e cartelle, i tag associati agli oggetti e gli elenchi di controllo degli accessi (). ACLs

Opzioni della modalità di trasferimento

È possibile configurare se DataSync trasferire solo i dati (inclusi i metadati) modificati dopo una copia iniziale o tutti i dati ogni volta che si esegue l'attività. Se hai intenzione di effettuare trasferimenti ricorrenti, potresti voler trasferire solo le modifiche apportate rispetto alla precedente esecuzione dell'attività.

Opzione nella console	Opzione nell'API	Descrizione
Trasferisci solo i dati che sono stati modificati	TransferModeimpostato su `CHANGED`	Dopo il trasferimento completo iniziale, DataSync copia solo i dati e i metadati che differisc ono tra la posizione di origine e quella di destinazione.
Trasferisci tutti i dati	TransferModeimpostato su `ALL`	DataSync copia tutto ciò che si trova nell'origine nella destinazione senza confronta re le differenze tra le posizioni.

Opzioni di gestione di file e oggetti

È possibile controllare alcuni aspetti del DataSync trattamento dei file o degli oggetti nella posizione di destinazione. Ad esempio, DataSync puoi eliminare file nella destinazione che non si trovano nell'origine.

Opzione nella console	Opzione nell'API	Descrizione
Conserva i file eliminati	PreserveDeletedFiles	Speciifica se DataSync mantiene file o oggetti nella posizione di destinazione che non esistono nell'origine. Se configuri la tua attività per eliminare oggetti dal tuo bucket Amazon S3, potresti incorrere in costi minimi per la durata dello storage per determinate classi di storage. Per informazioni dettagliate, consulta Considerazioni sulla classe di storage con Amazon S3 Transfers. **Warning** Non puoi configurare l'attività per eliminare i dati nella destinazione e trasferire anche tutti i dati. Quando trasferis ci tutti i dati, DataSync non scansiona la posizione di destinazi one e non sa cosa eliminare.
Sovrascrivi file	OverwriteMode	Speciifica se DataSync modifica i dati nella posizione di destinazione quando i dati o i metadati di origine sono cambiati. Se non configuri

Opzione nella console	Opzione nell'API	Descrizione
		l'attività per sovrascrivere i dati, i dati di destinazione non vengono sovrascritti anche se i dati di origine sono diversi. Se l'attività sovrascrive gli oggetti, potrebbero essere applicati costi aggiuntivi per determinate classi di archiviazione (ad esempio, per il recupero o l'eliminazione anticipata). Per informazioni dettagliate, consulta Considerazioni sulla classe di storage con Amazon S3 Transfers.

Opzioni di gestione dei metadati

DataSync può conservare i metadati di file e oggetti durante un trasferimento. I metadati che è DataSync possibile conservare dipendono dai sistemi di storage coinvolti e dal fatto che tali sistemi utilizzino una struttura di metadati simile.

Prima di configurare l'attività, assicuratevi di comprendere come vengono DataSync gestiti i metadati e i file speciali durante il trasferimento tra le posizioni di origine e di destinazione.

> **Important**
>
> DataSync supporta i trasferimenti da e verso determinati sistemi di archiviazione cloud di terze parti, come Google Cloud Storage e IBM Cloud Object Storage, che gestiscono i metadati di sistema in un modo che non è completamente compatibile con S3. Per questi trasferimenti, DataSync tenta di copiare attributi di metadati come`ContentType`, `ContentEncodingContentLanguage`, e `CacheControl` con la massima diligenza possibile. Se il sistema di storage di destinazione non applica questi attributi, questi verranno ignorati durante la verifica delle attività.

Opzione nella console	Opzione nell'API	Descrizione
Proprietà della copia	Gid e Uid	Speciifica se DataSync copia la proprietà di file e cartelle POSIX, ad esempio l'ID di gruppo dei proprietari del file e l'ID utente del proprietario del file.
Autorizzazioni di copia	PosixPermissions	Speciifica se DataSync copia le autorizzazioni POSIX per file e cartelle dall'origine alla destinazione.
Copia i timestamp	Atime e Mtime	Speciifica se DataSync copia i metadati del timestamp dall'origine alla destinazione. Richiesto quando è necessario eseguire un'attività più di una volta.
Copia i tag degli oggetti	ObjectTags	Speciifica se DataSync conserva i tag associati agli oggetti durante il trasferimento tra sistemi di archiviazione degli oggetti.
Proprietà della copia e DACLs SACLs	SecurityDescriptorCopyFlags impostato su `OWNER_DACL_SACL`	DataSync copia quanto segue: • Il proprietario dell'oggetto. • Liste di accesso discrezionali NTFS (DACLs), che determinano se concedere l'accesso a un oggetto. • Liste di controllo degli accessi al sistema NTFS (SACLs), utilizzate dagli

Opzione nella console	Opzione nell'API	Descrizione
		amministratori per registrare i tentativi di accesso a un oggetto protetto. Nota: non SACLs vengono copiati se si utilizza la versione 1.0 di SMB. La copia SACLs richiede DACLs la concessione di autorizzazioni specifiche all'utente Windows che DataSync utilizza SMB per accedere alla posizione dell'utente. Per ulteriori informazioni, consulta Creazione di una posizione per SMB, FSx per Windows File Server o FSx per ONTAP (a seconda del tipo di posizione nel trasferimento).
Proprietà della copia e DACLs	SecurityDescriptorCopyFlags impostato su `OWNER_DACL`	DataSync copia quanto segue: • Il proprietario dell'oggetto. • DACLs, che determinano se concedere l'accesso a un oggetto. DataSync non copierà SACLs quando scegli questa opzione.

Opzione nella console	Opzione nell'API	Descrizione
Non copiate la proprietà o ACLs	SecurityDescriptorCopyFlags impostato su NONE	DataSync non copia alcun dato sulla proprietà o sulle autorizzazioni. Gli oggetti che DataSync scrivono nella posizione di destinazione sono di proprietà dell'utente le cui credenziali sono state fornite per accedere DataSync alla destinazione. Le autorizzazioni degli oggetti di destinazione sono determinate in base alle autorizzazioni configurate sul server di destinazione.

Configurazione delle opzioni di gestione di file, oggetti e metadati

È possibile configurare la modalità di DataSync gestione di file, oggetti e metadati durante la creazione, la modifica o l'avvio dell'attività di trasferimento.

Utilizzo della console di DataSync

Le seguenti istruzioni descrivono come configurare le opzioni di gestione di file, oggetti e metadati durante la creazione di un'attività.

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per la modalità di trasferimento, scegli una delle seguenti opzioni:

   - Trasferisci solo i dati che sono stati modificati
   - Trasferisci tutti i dati

Per ulteriori informazioni su queste opzioni, consulta Opzioni della modalità di trasferimento.

5. Seleziona Mantieni file eliminati se desideri DataSync mantenere nella posizione di destinazione file o oggetti che non esistono nell'origine.

   Se non scegli questa opzione e la tua attività elimina oggetti dal tuo bucket Amazon S3, potresti incorrere in costi minimi per la durata dello storage per determinate classi di storage. Per informazioni dettagliate, consulta Considerazioni sulla classe di storage con Amazon S3 Transfers.

   > ⚠ Warning
   >
   > Non puoi deselezionare questa opzione e abilitare Trasferisci tutti i dati. Quando trasferisci tutti i dati, DataSync non scansiona la posizione di destinazione e non sa cosa eliminare.

6. Seleziona Sovrascrivi file se desideri DataSync modificare i dati nella posizione di destinazione quando i dati o i metadati di origine sono cambiati.

   Se l'attività sovrascrive gli oggetti, potrebbero essere applicati costi aggiuntivi per determinate classi di archiviazione (ad esempio, per il recupero o l'eliminazione anticipata). Per informazioni dettagliate, consulta Considerazioni sulla classe di storage con Amazon S3 Transfers.

   Se non scegli questa opzione, i dati di destinazione non vengono sovrascritti anche se i dati di origine sono diversi.

7. In Opzioni di trasferimento, seleziona il modo in cui desideri DataSync gestire i metadati. Per ulteriori informazioni su queste opzioni, consulta Opzioni di gestione dei metadati.

   > ⚠ Important
   >
   > Le opzioni visualizzate nella console dipendono dalle posizioni di origine e destinazione dell'attività. Potrebbe essere necessario espandere Impostazioni aggiuntive per visualizzare alcune di queste opzioni.

   - Proprietà della copia
   - Autorizzazioni di copia

- Copia i timestamp
- Copia i tag degli oggetti
- Proprietà delle copie e DACLs SACLs
- Proprietà della copia e DACLs
- Non copiare la proprietà o ACLs

Utilizzo dell' DataSync API

È possibile configurare le opzioni di gestione di file, oggetti e metadati utilizzando il `Options` parametro con una delle seguenti operazioni:

- CreateTask
- StartTaskExecution
- UpdateTask

Configurazione della modalità di AWS DataSync verifica dell'integrità dei dati

Durante un trasferimento, AWS DataSync utilizza la verifica tramite checksum per verificare l'integrità dei dati copiati tra le sedi. Puoi anche DataSync configurare l'esecuzione di ulteriori verifiche al termine del trasferimento.

Opzioni di verifica dei dati

Utilizza le seguenti informazioni per decidere se e come DataSync eseguire questi controlli aggiuntivi.

Opzione Console	Opzione API	Descrizione
Verifica solo i dati trasferiti (consigliato)	VerifyModeimpostato su `ONLY_FILES_TRANSFERRED`	DataSync calcola il checksum dei dati trasferiti (inclusi i metadati) nella posizione di origine. Al termine del trasferimento, DataSync confronta questo checksum con il checksum calcolato sugli stessi dati nella destinazione.

Opzione Console	Opzione API	Descrizione
		Consigliamo questa opzione per il trasferimento alle classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con Amazon S3 Transfers.

Opzione Console	Opzione API	Descrizione
Verifica tutti i dati	VerifyModeimpostato su `POINT_IN_TIME_CONSISTENT`	Al termine del trasferimento, DataSync controlla l'intera origine e la destinazione per verificare che entrambe le sedi siano completamente sincronizzate. **Note** Non supportato quando l'attività utilizza la modalità Avanzata. Se si utilizza un manifesto, analizza e verifica DataSync solo ciò che è elencato nel manifesto. Non puoi utilizzare questa opzione per il trasferimento a classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con Amazon S3 Transfers.

Opzione Console	Opzione API	Descrizione
Non verificare i dati dopo il trasferimento	VerifyModeimpostato su `NONE`	DataSync esegue controlli di integrità dei dati solo durante il trasferimento. A differenza di altre opzioni, non è prevista alcuna verifica aggiuntiva al termine del trasferimento.

Configurazione della verifica dei dati

È possibile configurare le opzioni di verifica dei dati quando si crea un'attività, si aggiorna un'attività o si avvia l'esecuzione di un'attività.

Utilizzo della console di DataSync

Le seguenti istruzioni descrivono come configurare le opzioni di verifica dei dati durante la creazione di un'attività.

Per configurare la verifica dei dati utilizzando la console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per la verifica, scegli una delle seguenti opzioni:

   - Verifica solo i dati trasferiti (scelta consigliata)
   - Verifica tutti i dati
   - Non verificare i dati dopo il trasferimento

Utilizzo dell'API DataSync

È possibile configurare la modalità di DataSync verifica dei dati utilizzando il `VerifyMode` parametro con una delle seguenti operazioni:

- CreateTask
- UpdateTask
- StartTaskExecution

Impostazione dei limiti di larghezza di banda per l'attività AWS DataSync

È possibile configurare i limiti di larghezza di banda di rete per la propria AWS DataSync attività e ciascuna delle sue esecuzioni.

> **Note**
>
> Non applicabile alle attività in modalità Avanzata.

Limitazione della larghezza di banda per un'attività

Imposta un limite di larghezza di banda durante la creazione, la modifica o l'avvio di un'attività.

Utilizzo della console di DataSync

Le seguenti istruzioni descrivono come configurare un limite di larghezza di banda per l'attività al momento della creazione.

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per Limite di larghezza di banda, scegli una delle seguenti opzioni:

   - Seleziona Usa disponibile per utilizzare tutta la larghezza di banda di rete disponibile per ogni esecuzione di attività.
   - Seleziona Imposta limite di larghezza di banda (MiB/s) e inserisci la larghezza di banda massima che desideri utilizzare DataSync per ogni esecuzione di attività.

Utilizzo dell'API DataSync

È possibile configurare il limite di larghezza di banda di un'attività utilizzando il `BytesPerSecond` parametro con una delle seguenti operazioni:

- CreateTask
- UpdateTask
- StartTaskExecution

Limitazione della larghezza di banda per l'esecuzione di un'attività

È possibile modificare il limite di larghezza di banda per l'esecuzione di un'attività in esecuzione o in coda.

Utilizzo della console di DataSync

1. Apri la console all' AWS DataSync indirizzo. https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione, espandi Trasferimento dati, quindi scegli Attività.
3. Scegli l'attività, quindi seleziona Cronologia per visualizzare le esecuzioni dell'attività.
4. Scegli l'esecuzione dell'attività che desideri modificare, quindi scegli Modifica.
5. Nella finestra di dialogo, scegliete una delle seguenti opzioni:
   - Seleziona Usa disponibile per utilizzare tutta la larghezza di banda di rete disponibile per l'esecuzione dell'attività.
   - Seleziona Imposta limite di larghezza di banda (MiB/s) e inserisci la larghezza di banda massima che desideri utilizzare DataSync per l'esecuzione dell'attività.
6. Scegli Save changes (Salva modifiche).

   Il nuovo limite di larghezza di banda entra in vigore entro 60 secondi.

Utilizzo dell'API DataSync

È possibile modificare il limite di larghezza di banda per l'esecuzione di un'operazione in esecuzione o in coda utilizzando il `BytesPerSecond` parametro associato all'operazione. UpdateTaskExecution

Pianificazione dell'esecuzione dell' AWS DataSync attività

È possibile impostare una pianificazione delle AWS DataSync attività per trasferire periodicamente i dati tra le posizioni di archiviazione.

Come funziona la pianificazione delle DataSync attività

Un' DataSync operazione pianificata viene eseguita a una frequenza specificata dall'utente, con un intervallo minimo di 1 ora. È possibile creare una pianificazione delle attività utilizzando espressioni cron o rate.

> **Important**
>
> Non è possibile pianificare l'esecuzione di un'attività a intervalli superiori a 1 ora.

Utilizzo delle espressioni cron

Usa le espressioni cron per le pianificazioni delle attività che vengono eseguite in un'ora e in un giorno specifici. Ad esempio, ecco come configurare una pianificazione delle attività AWS CLI che viene eseguita alle 12:00 UTC ogni domenica e mercoledì.

```
cron(0 12 ? * SUN,WED *)
```

Utilizzo delle espressioni di frequenza

Utilizza le espressioni di frequenza per le pianificazioni delle attività eseguite a intervalli regolari, ad esempio ogni 12 ore. Ad esempio, ecco come è possibile configurare una pianificazione delle attività AWS CLI che viene eseguita ogni 12 ore:

```
rate(12 hours)
```

> **Tip**
>
> Per ulteriori informazioni sulla sintassi delle espressioni cron e rate, consulta la Amazon EventBridge User Guide.

Creazione di una DataSync pianificazione delle attività

Puoi pianificare la frequenza di esecuzione dell'attività utilizzando la DataSync console o AWS CLI l' DataSync API.

Utilizzo della DataSync console

Le seguenti istruzioni descrivono come impostare una pianificazione durante la creazione di un'attività. È possibile modificare la pianificazione in un secondo momento durante la modifica dell'attività.

Nella console, alcune opzioni di pianificazione consentono di specificare l'ora esatta di esecuzione dell'attività (ad esempio ogni giorno alle 22:30). Se non includi un orario per queste opzioni, l'attività viene eseguita nel momento in cui l'hai creata (o aggiornata).

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Per la frequenza di pianificazione, esegui una delle seguenti operazioni:

   - Scegli Non pianificato se non desideri che l'attività venga eseguita secondo una pianificazione.
   - Scegli Ogni ora, quindi scegli il minuto durante l'ora in cui desideri che l'attività venga eseguita.
   - Scegli Ogni giorno e inserisci l'ora UTC in cui desideri che l'attività venga eseguita.
   - Scegli Settimanale e il giorno della settimana e inserisci l'ora UTC in cui desideri che l'attività venga eseguita.
   - Scegli Giorni della settimana, scegli uno o più giorni specifici e inserisci l'ora UTC in cui l'attività deve essere eseguita nel formato HH:MM.
   - Scegli Personalizzato, quindi seleziona Espressione Cron o Espressione velocità. Inserisci la pianificazione delle attività con un intervallo minimo di 1 ora.

Utilizzando il AWS CLI

È possibile creare una pianificazione per l' DataSync attività utilizzando il `--schedule` parametro con il `start-task-execution` comando `create-taskupdate-task`, o.

Le istruzioni seguenti descrivono come eseguire questa operazione con il `create-task` comando.

1. Copia il seguente `create-task` comando:

```
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. Per il `--source-location-arn` parametro, specifica l'Amazon Resource Name (ARN) della posizione da cui stai trasferendo i dati.
3. Per il `--destination-location-arn` parametro, specifica l'ARN della posizione in cui stai trasferendo i dati.
4. Per il `--schedule` parametro, specifica un'espressione cron o rate per la tua pianificazione.

   Nell'esempio, l'espressione cron *`cron(0 12 ? * SUN,WED *)`* imposta una pianificazione delle attività che viene eseguita alle 12:00 UTC ogni domenica e mercoledì.
5. Esegui il `create-task` comando per creare l'attività con la pianificazione.

Sospensione della pianificazione di un' DataSync attività

In alcuni casi è necessario sospendere la pianificazione delle DataSync attività. Ad esempio, potrebbe essere necessario disabilitare temporaneamente un trasferimento ricorrente per risolvere un problema relativo all'operazione o eseguire la manutenzione del sistema di storage.

DataSync potrebbe disattivare automaticamente la pianificazione delle attività per i seguenti motivi:

- L'operazione fallisce ripetutamente con lo stesso errore.
- Si disattiva Regione AWS un elemento utilizzato dall'attività.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività.

3. Scegli l'attività per la quale desideri sospendere la pianificazione, quindi scegli Modifica.
4. Per Pianificazione, disattiva Abilita pianificazione. Scegli Save changes (Salva modifiche).

Usando il AWS CLI

1. Copia il seguente `update-task` comando:

```
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. Per il `--task-arn` parametro, specificate l'ARN dell'attività per la quale desiderate sospendere la pianificazione.
3. Per il `--schedule` parametro, effettuate le seguenti operazioni:
   - Per`ScheduleExpression`, specifica un'espressione cron o rate per la tua pianificazione.

     Nell'esempio, l'espressione *`cron(0 12 ? * SUN,WED *)`* imposta una pianificazione delle attività che viene eseguita alle 12:00 UTC ogni domenica e mercoledì.
   - Per`Status`, specificare di `DISABLED` sospendere la pianificazione delle attività.
4. Esegui il comando `update-task`.
5. Per riprendere la pianificazione, esegui lo stesso `update-task` comando con `Status` set to. `ENABLED`

Verifica dello stato di una pianificazione delle DataSync attività

Puoi vedere se la pianificazione delle DataSync attività è abilitata.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività.
3. Nella colonna Pianificazione, controlla se la pianificazione dell'attività è abilitata o disabilitata.

Usando il AWS CLI

1. Copia il seguente `describe-task` comando:

```
aws datasync describe-task \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

2. Per il `--task-arn` parametro, specifica l'ARN dell'attività su cui desideri informazioni.
3. Esegui il comando `describe-task`.

Riceverai una risposta che fornisce dettagli sull'attività, inclusa la pianificazione. (L'esempio seguente si concentra principalmente sulla configurazione della pianificazione delle attività e non mostra una `describe-task` risposta completa).

L'esempio mostra che la pianificazione dell'attività è disabilitata manualmente. Se la pianificazione è disattivata da DataSync `SERVICE`, viene visualizzato un messaggio di errore per aiutarti `DisabledReason` a capire perché l'attività continua a fallire. Per ulteriori informazioni, consulta ???.

```
{
    "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."
    },
    ...
}
```

Taggare le attività AWS DataSync

I tag sono coppie chiave-valore che ti aiutano a gestire, filtrare e cercare le tue AWS DataSync risorse. È possibile aggiungere fino a 50 tag a ciascuna DataSync attività ed esecuzione.

Ad esempio, è possibile creare un'attività per una migrazione di dati di grandi dimensioni e etichettarla con la chiave **`Project`** e il valore**`Large Migration`**. Per organizzare ulteriormente la migrazione, puoi etichettare un'esecuzione dell'attività con la chiave **`Transfer Date`** e il valore **`May`**

`2021` (le esecuzioni di attività successive potrebbero essere **`June 2021`** contrassegnate e così via). **`July 2021`**

Taggare l'attività DataSync

Puoi etichettare l' DataSync attività solo durante la creazione dell'attività.

Utilizzo della console di DataSync

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Nella pagina Configura impostazioni, scegli Aggiungi nuovo tag per etichettare l'attività.

Usando il AWS CLI

1. Copia il seguente `create-task` comando:

```
aws datasync create-task \
    --source-location-arn 'arn:aws:datasync:region:account-id:location/source-location-id' \
    --destination-location-arn 'arn:aws:datasync:region:account-id:location/destination-location-id' \
    --tags Key=tag-key,Value=tag-value
```

2. Specificate i seguenti parametri nel comando:

   - `--source-location-arn`— Specificare l'Amazon Resource Name (ARN) della posizione di origine del trasferimento.
   - `--destination-location-arn`— Specificare l'ARN della località di destinazione nel trasferimento.
   - `--tags`— Specificare i tag che si desidera applicare all'attività.

     Per più di un tag, separa ogni coppia chiave-valore con uno spazio.
3. (Facoltativo) Specificate altri parametri che abbiano senso per lo scenario di trasferimento.

Per un elenco di`--options`, vedete il comando create-task.

4. Esegui il comando `create-task`.

   Viene visualizzata una risposta che mostra l'attività appena creata.

```
{
    "TaskArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

Per visualizzare i tag che hai aggiunto a questa attività, puoi usare il list-tags-for-resourcecomando.

Etichettare l'esecuzione dell' DataSync attività

Puoi etichettare ogni esecuzione della tua DataSync attività.

Se l'attività contiene già dei tag, ricorda quanto segue sull'utilizzo dei tag nelle esecuzioni delle attività:

- Se si avvia l'operazione con la console, i tag creati dall'utente vengono applicati automaticamente all'esecuzione dell'operazione. Tuttavia, i tag creati dal sistema che iniziano con non `aws:` vengono applicati.
- Se si avvia l'attività con l' DataSync API o AWS CLI i relativi tag non vengono applicati automaticamente all'esecuzione dell'attività.

Utilizzo della console di DataSync

Per aggiungere, modificare o rimuovere tag dall'esecuzione di un'attività, è necessario avviare l'attività con opzioni di sovrascrittura.

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività.
3. Scegli l'attività.
4. Scegli Start, quindi scegli una delle seguenti opzioni:

   - Inizia con i valori predefiniti: applica tutti i tag associati all'attività.

- Inizia con l'override delle opzioni: consente di aggiungere, modificare o rimuovere tag per l'esecuzione di questa particolare attività.

Usando il AWS CLI

1. Copia il seguente `start-task-execution` comando:

```
aws datasync start-task-execution \
    --task-arn 'arn:aws:datasync:region:account-id:task/task-id' \
    --tags Key=tag-key,Value=tag-value
```

2. Specificate i seguenti parametri nel comando:

   - `--task-arn`— Specificare l'ARN dell'attività che si desidera avviare.
   - `--tags`— Specificate i tag da applicare a questa esecuzione specifica dell'attività.

     Per più di un tag, separa ogni coppia chiave-valore con uno spazio.

3. (Facoltativo) Specificate altri parametri che abbiano senso per la vostra situazione.

   Per ulteriori informazioni, consulta il comando start-task-execution.

4. Esegui il comando `start-task-execution`.

   Viene visualizzata una risposta che mostra l'esecuzione dell'attività appena avviata.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

Per visualizzare i tag che hai aggiunto a questa attività, puoi usare il list-tags-for-resourcecomando.

Avvio di un'attività per trasferire i dati

Una volta creata l'attività di AWS DataSync trasferimento, puoi iniziare a spostare i dati. Ogni esecuzione di un'attività è denominata esecuzione dell'attività. Per informazioni su ciò che accade durante l'esecuzione di un'attività, vedereCome DataSync trasferisce file, oggetti e directory.

> **Important**
>
> Se hai intenzione di trasferire dati da o verso una sede Amazon S3, consulta in che modo DataSync possono influire sui costi delle richieste S3 e sulla pagina dei DataSync prezzi prima di iniziare.

Avvio della tua attività

Dopo aver creato l'attività, puoi iniziare subito a spostare i dati.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività.
3. Scegli l'attività che desideri eseguire.

   Assicurati che l'attività abbia lo stato Disponibile. Puoi anche selezionare più attività.
4. Scegli Azioni, quindi scegli una delle seguenti opzioni:

   - Avvia: esegue l'attività (o le attività se ne hai selezionate più di una).
   - Inizia con l'override delle opzioni: consente di modificare alcune impostazioni delle attività prima di iniziare a spostare i dati. Quando sei pronto, scegli Avvia.
5. Scegli Visualizza i dettagli dell'esecuzione per visualizzare i dettagli sull'esecuzione dell'attività in esecuzione.

Utilizzando il AWS CLI

Per avviare l' DataSync attività, è sufficiente specificare l'Amazon Resource Name (ARN) dell'attività che si desidera eseguire. Ecco un `start-task-execution` comando di esempio:

```
aws datasync start-task-execution \
    --task-arn 'arn:aws:datasync:region:account-id:task/task-id'
```

L'esempio seguente avvia un'attività con alcune impostazioni diverse da quelle predefinite dell'attività:

```
aws datasync start-task-execution \
```

```
    --override-options VerifyMode=NONE,OverwriteMode=NEVER,PosixPermissions=NONE
```

Il comando restituisce un ARN per l'esecuzione dell'attività simile all'esempio seguente:

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:209870788375:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

> **Note**
>
> Ogni agente può eseguire una singola attività alla volta.

Utilizzo dell'API DataSync

È possibile avviare l'attività utilizzando l'StartTaskExecutionoperazione. Utilizzare l'DescribeTaskExecutionoperazione per ottenere dettagli sull'esecuzione dell'attività in esecuzione.

Una volta avviata, puoi controllare lo stato di esecuzione dell'attività mentre DataSync copi i tuoi dati. Se necessario, puoi anche limitare la larghezza di banda dell'esecuzione dell'attività.

Stati di esecuzione delle attività

Quando si avvia un' DataSync attività, è possibile che vengano visualizzati questi stati. (Gli stati delle attività sono diversi dagli stati di esecuzione delle attività.)

Stato della console	Stato dell'API	Descrizione
In coda	`QUEUED`	L'esecuzione di un'altra attività è in esecuzione e utilizza lo stesso DataSync agente. Per ulteriori informazioni, consulta Sapere quando l'attività è in coda.
Avvio	`LAUNCHING`	DataSync sta inizializzando l'esecuzione dell'attività. Questo stato in genere passa rapidamente, ma può richiedere fino a qualche minuto.
Lanciato	`LAUNCHED`	DataSync ha avviato l'esecuzione dell'attività.

Stato della console	Stato dell'API	Descrizione
Preparing (Preparazione)	`PREPARING`	DataSync sta determinando quali dati trasferire. La preparazione può richiedere solo pochi minuti, alcune ore o anche di più, a seconda del numero di file, oggetti o directory in entrambe le posizioni e della configurazione dell'attività. Il funzionamento della preparazione dipende anche dalla modalità di operazione. Per ulteriori informazioni, consulta Come si DataSync prepara il trasferimento dei dati.
Trasferimento	`TRANSFERRING`	DataSync sta effettuando il trasferimento effettivo dei dati.
Verifica in corso	`VERIFYING`	DataSync sta verificando l'integrità dei dati al termine del trasferimento.
Riuscito	`SUCCESS`	L'esecuzione dell'operazione è riuscita.
Annullamento in corso	`CANCELLING`	L'esecuzione dell'attività è in fase di annullamento.
Errore	`ERROR`	L'esecuzione dell'operazione non è riuscita.

Sapere quando l'attività è in coda

Quando si eseguono più attività (ad esempio, si trasferisce un set di dati di grandi dimensioni), è DataSync possibile mettere in coda le attività da eseguire in serie (first in, first out). Alcuni esempi di quando ciò accade includono:

- Eseguite diverse attività che utilizzano lo stesso DataSync agente. Sebbene sia possibile utilizzare lo stesso agente per più attività, un agente può eseguire solo un'attività alla volta.
- È in corso l'esecuzione di un'attività e si avviano esecuzioni aggiuntive della stessa attività utilizzando filtri o manifesti diversi.

In ogni esempio, le attività in coda non iniziano fino al termine dell'attività che le precede.

Annullamento dell'esecuzione dell'attività

È possibile interrompere l'esecuzione di qualsiasi attività in esecuzione o in coda. DataSync

Per annullare l'esecuzione di un'operazione utilizzando la console

1. Aprire la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività.
3. Seleziona l'ID attività per l'attività in esecuzione che desideri monitorare.

   Lo stato dell'attività deve essere In esecuzione.
4. Scegli Cronologia per visualizzare le esecuzioni dell'attività.
5. Seleziona l'esecuzione dell'attività che desideri interrompere, quindi scegli Interrompi.
6. Nella finestra di dialogo, scegliete Stop.

Per annullare un'operazione in esecuzione o in coda utilizzando l' DataSync API, consulta. CancelTaskExecution

Annullamento automatico delle attività bloccate

A volte l'esecuzione di un' DataSync attività in esecuzione può bloccarsi.

Monitoraggio dei AWS DataSync trasferimenti

Il monitoraggio è importante per mantenere l'affidabilità e le prestazioni delle attività di AWS DataSync trasferimento. Ti consigliamo di raccogliere i dati di monitoraggio in modo da poter eseguire più facilmente il debug degli eventuali errori. Prima di iniziare il monitoraggio DataSync, tuttavia, crea un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

AWS fornisce vari servizi e strumenti per il monitoraggio DataSync. Alcuni di questi possono essere configurati in modo che eseguano il monitoraggio al posto tuo, mentre altri richiedono un intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Argomenti

- Comprensione dei contatori delle prestazioni di trasferimento dati
- Monitoraggio dei trasferimenti di dati con i CloudWatch parametri di Amazon
- Monitoraggio dei trasferimenti di dati con report sulle attività
- Monitoraggio dei trasferimenti di dati con Amazon CloudWatch Logs
- Registrazione delle chiamate AWS DataSync API con AWS CloudTrail
- Monitoraggio degli eventi tramite Amazon EventBridge
- Monitoraggio AWS DataSync con strumenti manuali

Comprensione dei contatori delle prestazioni di trasferimento dati

Quando si avvia un'attività, AWS DataSync fornisce contatori che aiutano a tenere traccia delle prestazioni e dei progressi del trasferimento dei dati.

Utilizzate le seguenti informazioni per capire cosa rappresenta ogni contatore. Puoi visualizzare questi contatori nella DataSync console o in una DescribeTaskExecutionrisposta. Alcuni contatori non sono disponibili in tutte le modalità di attività.

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
–	`BytesWritten`	Avanzato, di base	Il numero di byte logici che vengono DataSync effettivamente scritti nella posizione di destinazione.
Velocità effettiva dei dati	–	Migliorato, di base	La velocità di DataSync scrittura dei byte logici nella posizione di destinazione. Se si utilizza DescribeTaskExecution, il modo in cui si calcola questo contatore dipende dalla modalità di operazione in uso: • Modalità avanzata: Dividi `BytesWritten` per `TotalDuration` • Modalità base: Dividi `BytesWritten` per `TransferDuration`

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Dati trasferiti	`BytesTransferred`	Avanzato, di base	Il numero di byte DataSync inviati alla rete prima della compressione (se la compressione è possibile). Per il numero di byte trasferiti sulla rete, consultate il contatore della velocità di trasmissione di rete (nella console) o `BytesCompressed` (in DescribeTaskExecution).

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Eliminato dalla destinazione	`FilesDeleted`	Avanzato, di base	Il numero di file, oggetti e directory DataSync effettivamente eliminati nella posizione di destinazione. Se non configuri l'attività per eliminare i dati nella destinazione che non si trovano nell'origine: • L'eliminazione dalla destinazione non viene visualizzata nella console. • `FilesDeleted` mostra sempre il valore di `0`.
–	`EstimatedBytesToTransfer`	Avanzato, di base	Il numero di byte logici che DataSync prevede di scrivere nella posizione di destinazione.

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
–	`EstimatedFilesToDelete`	Avanzato, di base	Il numero di file, oggetti e directory che DataSync prevede di eliminare nella posizione di destinazione. Se non configuri l'attività per eliminare i dati nella destinazione che non si trovano nell'origine, il valore è sempre. `0`

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
–	`EstimatedFilesToTransfer`	Avanzato, di base	Il numero di file, oggetti e directory che DataSync prevede di trasferire sulla rete. Questo valore viene calcolato durante la DataSync preparazione del trasferimento. Il modo in cui viene calcolato dipende principalmente dalla modalità di trasferimento utilizzata: • Se la modalità di trasferimento è impostata per trasferire solo i dati modificati: il calcolo si basa sul confronto del contenuto delle posizioni di origine e di destinazione e sulla determinazione della differenza da trasferire. La differenza può includere: • Tutto ciò che viene aggiunto o modificato

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
			nella posizione di origine. • Tutto ciò che si trova in entrambe le posizioni e modificato nella destinazione dopo un trasferimento iniziale (a meno che non si configuri l'attività in modo da non sovrascrivere i dati nella destinazione). • (Solo modalità base) Il numero di elementi che DataSync prevede di eliminare (se si configura l'attività per eliminare i dati nella destinazione). • Se la modalità di trasferimento è impostata per trasferire tutti i dati: il calcolo si basa solo sugli elementi che DataSync

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
			si trovano nella posizione di origine.
Velocità effettiva dei file	–	Avanzato, di base	La velocità di DataSync trasferimento di file, oggetti e directory sulla rete. Se si utilizza DescribeTaskExecution, il modo in cui si calcola questo contatore dipende dalla modalità di operazione in uso: • Modalità avanzata: Dividi `FilesTransferred` per `TotalDuration` • Modalità base: Dividi `FilesTransferred` per `TransferDuration`

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
–	`FilesFailed`	Migliorata	Il numero di oggetti che DataSync non vengono preparati , trasferiti, verificati ed eliminati durante l'esecuzione dell'attività. In caso di errori, è possibile visualizzarli rispettivamente accanto ai contatori Preparati, Trasferiti, Ignorati ed Eliminati dalla console di destinazione.

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Elencato alla fonte	`FilesListed.AtSource`	Migliorato	Il numero di oggetti DataSync trovati nella posizione di origine. • Con un manifesto, DataSync elenca solo ciò che è nel manifesto (e non tutto nella posizione di origine). • Con un filtro di inclusione, DataSync elenca solo ciò che corrisponde al filtro nella posizione di origine. • Con un filtro di esclusione, DataSync elenca tutto nella posizione di origine prima di applicare il filtro.

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
–	`FilesListed.AtDestinationForDelete`	Migliorato	Il numero di oggetti che DataSync si trovano nella posizione di destinazione. Questo contatore è applicabile solo se si configura l'attività per eliminare i dati nella destinazione che non si trovano nell'origine.

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Throughput di rete*	`BytesCompressed`	Avanzato, di base	Il numero di byte fisici DataSync trasferiti sulla rete dopo la compressione (se la compressione è possibile). Questo numero è in genere inferiore ai dati trasferiti (nella console) o `BytesTransferred` (in DescribeTaskExecution), a meno che i dati non siano comprimibili. * — Per la modalità avanzata, la velocità effettiva di rete non viene visualizzata nella console.

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Percentuale di compressione	–	Base	La percentuale di dati di trasferimento DataSync compressi prima dell'invio in rete. Se stai usando DescribeTaskExecution, puoi calcolare questo contatore con `1 - BytesCompressed / BytesWritten` .

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Preparato	`FilesPrepared`	Migliorato	Il numero di oggetti che DataSync tenteranno di trasferire dopo aver confrontato le posizioni di origine e di destinazione. Nella console, questo contatore può anche mostrare il numero di oggetti che vengono DataSync ignorati durante la preparazione. Per ulteriori informazioni, consulta Come si DataSync prepara il trasferimento dei dati. Questo contatore non è applicabile se si configura l'attività per trasferire tutti i dati. In questo scenario, DataSync copia tutto dall'origine alla destinazione senza confrontare le differenze tra le posizioni.

Console	**`DescribeTaskExecution`**	Supporto per la modalità Task	Descrizione
Velocità di elaborazione	–	Migliorato, di base	La velocità di DataSync lettura di file, oggetti e directory nella posizione di origine. La velocità di elaborazione si basa su diverse CloudWatch metriche. Le metriche esatte dipendono dalla modalità di attività utilizzata. Modalità avanzata: • `FilesListedSource` • `FilesPrepared` • `FilesTransferred` • `FilesVerified` Modalità base: • `FilesPreparedSource` • `FilesPreparedDestination` • `FilesTransferred`

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
			• `FilesVerifiedSource` • `FilesVerifiedDestination`
Rimanente	–	Base	Il numero rimanente di file, oggetti e directory che DataSync prevede di trasferire sulla rete. Se stai usando DescribeTaskExecution, puoi calcolare questo contatore `FilesTransferred` sottraendo da. `EstimatedFilesToTransfer`

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Ignorato *	`FilesSkipped`	Avanzato, di base	Il numero di file, oggetti e directory che vengono DataSync ignorati durante il trasferimento. * — In modalità avanzata, Skipped non viene visualizzato nella console. Invece, gli elementi ignorati vengono inclusi nel contatore Preparato quando si trasferiscono solo i dati che sono stati modificati o nel contatore Trasferito quando si trasferiscono tutti i dati.

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
Trasferiti	`FilesTransferred`	Migliorato, di base	Il numero di file, oggetti e directory che vengono DataSync trasferiti sulla rete. Questo valore viene aggiornato periodicamente durante l'esecuzione dell'attività quando qualcosa viene letto dall'origine e inviato in rete. Se DataSync non riesce a trasferire qualcosa, questo valore può essere inferiore a `EstimatedFilesToTransfer`. In alcuni casi, questo valore può anche essere maggiore di `EstimatedFilesToTransfer`. Questo contatore è specifico dell'implementazione per alcuni tipi di località, quindi non utilizzarlo come indicazione esatta di ciò che viene trasferito o per monitorare

Console	**DescribeTaskExecution**	Supporto per la modalità Task	Descrizione
			l'esecuzione delle attività. Nella console, questo contatore può anche mostrare il numero di oggetti che vengono DataSync ignorati durante il trasferim ento di un'operazione in modalità avanzata. Per ulteriori informazi oni, consulta Come DataSync trasferisce i tuoi dati.
Verificato	`FilesVerified`	Migliorato, di base	Il numero di file, oggetti e directory che viene DataSync verificato durante il trasferimento. Quando configuri l'attività in modo da verificare solo i dati trasferiti, in alcune situazioni DataSync non verifica le directory o i file o gli oggetti che non vengono trasferiti.

Monitoraggio dei trasferimenti di dati con i CloudWatch parametri di Amazon

Amazon CloudWatch fornisce metriche per monitorare le prestazioni di DataSync trasferimento e risolvere i problemi relativi all'attività di trasferimento.

Puoi monitorare le prestazioni AWS DataSync di trasferimento utilizzando i CloudWatch parametri di Amazon. DataSync i parametri vengono inviati automaticamente CloudWatch a intervalli di 5 minuti (indipendentemente da come configuri la registrazione). Le metriche vengono conservate per un periodo di 15 mesi.

Per visualizzare le CloudWatch metriche di DataSync, puoi utilizzare i seguenti strumenti:

- La console CloudWatch
- La CloudWatch CLI
- L' CloudWatch API
- La DataSync console (nella pagina dei dettagli dell'esecuzione dell'attività)

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

CloudWatch metriche per DataSync

DataSync le metriche utilizzano lo spazio dei `aws/datasync` nomi e forniscono metriche per le seguenti dimensioni:

- AgentId— L'ID univoco dell'agente (se l'attività utilizza un agente).
- TaskId— L'ID univoco dell'attività. Presenta il formato `task-`*`01234567890abcdef`*.

Lo spazio dei nomi `aws/datasync` include i parametri descritti di seguito. Alcune metriche non sono disponibili in tutte le modalità di attività.

CloudWatch parametro	Supporto per la modalità Task	Descrizione
`BytesCompressed`	Base	Il numero di byte fisici DataSync trasferiti sulla rete dopo la compressione (se la compressione è possibile

CloudWatch parametro	Supporto per la modalità Task	Descrizione
		). Questo numero è in genere inferiore `BytesTransferred` a quello a meno che i dati non siano comprimibili. Unità: byte
`BytesPreparedDestination`	Base	Il numero di byte logici DataSync preparati nella posizione di destinazione. Unità: byte
`BytesPreparedSource`	Base	Il numero di byte logici che vengono DataSync preparati nella posizione di origine. Unità: byte
`BytesTransferred`	Base	Il numero di byte DataSync inviati alla rete prima della compressione (se la compressione è possibile). Per il numero di byte trasferiti sulla rete, consulta la `BytesCompressed` metrica. Unità: byte
`BytesVerifiedDestination`	Base	Il numero di byte logici che viene DataSync verificato nella posizione di destinazione. Unità: byte
`BytesVerifiedSource`	Base	Il numero di byte logici che viene DataSync verificato nella posizione di origine. Unità: byte
`BytesWritten`	Avanzato, di base	Il numero di byte logici che vengono DataSync scritti nella posizione di destinazione. Unità: byte

CloudWatch parametro	Supporto per la modalità Task	Descrizione
`FilesDeleted`	Avanzato, di base	Il numero di file, oggetti e directory che vengono DataSync eliminati nella posizione di destinazione. Se non configuri l'attività per eliminare i dati nella destinazione che non si trovano nell'origine, il valore è sempre. `0` Unità: numero
`FilesListedSource`	Migliorato	Il numero di oggetti DataSync trovati nella posizione di origine. Unità: numero
`FilesPrepared`	Migliorato	Il numero di oggetti che DataSync tenteranno di trasferire e dopo aver confrontato le posizioni di origine e di destinazione. Per ulteriori informazioni, consulta Come si DataSync prepara il trasferimento dei dati. Questa metrica non è applicabile se configuri l'attività per trasferire tutti i dati. In questo scenario, DataSync copia tutto dall'origine alla destinazione senza confrontare le differenze tra le posizioni. Unità: numero
`FilesPreparedDestination`	Base	Il numero di file, oggetti e directory che vengono DataSync preparati nella posizione di destinazione. Unità: numero
`FilesPreparedSource`	Base	Il numero di file, oggetti e directory che vengono DataSync preparati nella posizione di origine. Unità: numero

CloudWatch parametro	Supporto per la modalità Task	Descrizione
`FilesSkipped`	Base	Il numero di file, oggetti e directory che vengono DataSync ignorati durante il trasferimento. Unità: numero
`FilesTransferred`	Avanzato, di base	Il numero di file, oggetti e directory che vengono DataSync trasferiti sulla rete. Questo valore viene aggiornato periodicamente durante l'esecuzione dell'attività quando qualcosa viene letto dall'origine e inviato in rete. **Note** Questo valore può essere inferiore `EstimatedFilesToTransfer` a quello di una DescribeTaskExecutionrisposta se DataSync non riesce a trasferire qualcosa. In alcuni casi, questo valore può anche essere maggiore di`EstimatedFilesToTransfer`. Questa metrica è specifica dell'implementazione per alcuni tipi di località, quindi non utilizzatela come indicazione esatta di ciò che è stato trasferito o per monitorare l'esecuzione delle attività. Unità: numero
`FilesVerified`	Migliorata	Il numero di oggetti che viene DataSync verificato durante il trasferimento. Unità: numero

CloudWatch parametro	Supporto per la modalità Task	Descrizione
`FilesVerifiedDestination`	Base	Il numero di file, oggetti e directory che viene DataSync verificato nella posizione di destinazione. Unità: numero
`FilesVerifiedSource`	Base	Il numero di file, oggetti e directory che viene DataSync verificato nella posizione di origine. Unità: numero

Monitoraggio dei trasferimenti di dati con report sulle attività

I report sulle attività forniscono informazioni dettagliate su quali AWS DataSync tentativi di trasferire, ignorare, verificare ed eliminare durante l'esecuzione di un'attività. Per ulteriori informazioni, consulta Come DataSync trasferisce file, oggetti e directory.

I report sulle attività vengono generati in formato JSON. Puoi personalizzare il livello di dettaglio nei tuoi report:

- I report sulle attività di solo riepilogo forniscono i dettagli necessari sull'esecuzione delle attività, ad esempio il numero di file trasferiti e l' DataSync eventuale possibilità di verificare l'integrità dei dati di tali file.
- I report sulle attività standard includono un riepilogo e report dettagliati che elencano ogni file, oggetto o cartella che DataSync tenta di trasferire, ignorare, verificare ed eliminare. Con un rapporto sulle attività standard, puoi anche specificare il livello del rapporto in modo da mostrare solo gli errori di esecuzione dell'attività o i relativi successi ed errori.

Casi d'uso

Ecco alcune situazioni in cui i report sulle attività possono aiutarti a monitorare e controllare i trasferimenti di dati:

- Quando esegui la migrazione di milioni di file, identifica rapidamente i file che DataSync presentano problemi di trasferimento.

- Verifica chain-of-custody i processi per i tuoi file.

Riepilogano solo i rapporti sulle attività

Un rapporto che è solo un riepilogo dell'esecuzione di un'attività include i seguenti dettagli:

- Il Account AWS che ha eseguito l'esecuzione dell'attività
- Le posizioni di origine e di destinazione
- Il numero totale di file, oggetti e cartelle che sono stati ignorati, trasferiti, verificati ed eliminati
- Il totale dei byte (logici e fisici) trasferiti
- Se l'esecuzione dell'attività è stata completata, annullata o si è verificato un errore
- L'ora di inizio e di fine (incluso il tempo totale del trasferimento)
- Le impostazioni dell'attività (come i limiti della larghezza di banda, la verifica dell'integrità dei dati e altre opzioni per il DataSync trasferimento)

Rapporti sulle attività standard

Un rapporto sulle attività standard include un riepilogo dell'esecuzione delle attività e rapporti dettagliati su ciò che DataSync tenta di trasferire, ignorare, verificare ed eliminare.

Argomenti

- Livello di rapporto
- Rapporti trasferiti
- Rapporti ignorati
- Rapporti verificati
- Rapporti eliminati

Livello di rapporto

Con i report sulle attività standard, puoi scegliere uno dei seguenti livelli di rapporto:

- Solo errori
- Successi ed errori (essenzialmente un elenco di tutto ciò che è accaduto durante l'esecuzione dell'attività)

Ad esempio, potresti voler vedere quali file sono DataSync stati ignorati correttamente durante il trasferimento e quali no. I file DataSync ignorati con successo potrebbero essere quelli che desideri DataSync escludere di proposito perché esistono già nella posizione di destinazione. Tuttavia, un errore ignorato, ad esempio, potrebbe indicare che DataSync non dispone delle autorizzazioni necessarie per leggere un file.

Rapporti trasferiti

Un elenco di file, oggetti e directory che DataSync hanno tentato di trasferire durante l'esecuzione dell'attività. Un rapporto trasferito include i seguenti dettagli:

- I percorsi per i dati trasferiti
- Cosa è stato trasferito (contenuto, metadati o entrambi)
- I metadati, che includono il tipo di dati, la dimensione del contenuto (solo oggetti e file) e altro
- L'ora in cui un elemento è stato trasferito
- La versione dell'oggetto (se la destinazione è un bucket Amazon S3 con il controllo delle versioni abilitato)
- Se qualcosa è stato sovrascritto nella destinazione
- Se un articolo è stato trasferito correttamente

> **Note**
>
> Quando sposti dati tra i bucket S3, il prefisso che specifichi nella posizione di origine può essere visualizzato nel report (o nei CloudWatch log di Amazon), anche se tale prefisso non esiste come oggetto nella posizione di destinazione. (Nella DataSync console, potresti anche notare che questo prefisso viene visualizzato come dati ignorati o verificati.)

Rapporti ignorati

Un elenco di file, oggetti e directory che DataSync si trovano nella posizione di origine ma che non sono stati trasferiti. I motivi per cui i DataSync dati vengono ignorati possono dipendere da diversi fattori, come la configurazione delle attività e le autorizzazioni del sistema di storage. Ecco alcuni esempi:

- Esiste un file nelle posizioni di origine e di destinazione. Il file nell'origine non è stato modificato dall'esecuzione dell'attività precedente. Poiché stai trasferendo solo dati che sono stati modificati, DataSync non trasferisce quel file la prossima volta che esegui l'operazione.
- Un oggetto che esiste in entrambe le posizioni cambia nella fonte. Quando esegui l'attività, DataSync salta questo oggetto nella destinazione perché l'attività non sovrascrive i dati nella destinazione.
- DataSync ignora un oggetto nell'origine che utilizza una classe di archiviazione e non viene ripristinato. È necessario ripristinare un oggetto archiviato per poterlo DataSync leggere.
- DataSync salta un file, un oggetto o una directory nella posizione di origine perché non può leggerlo. Se ciò accade e non è previsto, controlla le autorizzazioni di accesso dello spazio di archiviazione e assicurati che sia DataSync possibile leggere ciò che è stato ignorato.

Un rapporto ignorato include i seguenti dettagli:

- I percorsi per i dati ignorati
- L'ora in cui un elemento è stato ignorato
- Il motivo per cui è stato ignorato
- Se un elemento è stato ignorato con successo

> **Note**
>
> I report ignorati possono essere di grandi dimensioni quando includono successi ed errori, se si configura l'attività in modo da trasferire solo i dati modificati e i dati di origine esistono già nella destinazione.

Rapporti verificati

Un elenco di file, oggetti e directory che DataSync hanno tentato di verificare l'integrità durante l'esecuzione dell'attività. Un rapporto sui dati verificati include i seguenti dettagli:

- I percorsi per i dati verificati
- L'ora in cui un articolo è stato verificato
- Il motivo dell'errore di verifica (se presente)
- I SHA256 checksum di origine e destinazione (solo file)

- Se un articolo è stato verificato con successo

Tieni presente quanto segue sui report verificati:

- Quando configuri l'attività in modo da verificare solo i dati trasferiti, in alcune situazioni DataSync non verifica le directory o i file o gli oggetti che non vengono trasferiti. In entrambi i casi, DataSync non include dati non verificati in questo rapporto.
- Se utilizzi la modalità Avanzata, la verifica potrebbe richiedere più tempo del solito se trasferisci oggetti di grandi dimensioni.

Rapporti eliminati

Un elenco di file, directory e oggetti che sono stati eliminati durante l'esecuzione dell'attività. DataSync genera questo rapporto solo se si configura l'attività in modo da eliminare i dati nella posizione di destinazione che non si trova nell'origine. Un rapporto sui dati eliminati include i seguenti dettagli:

- I percorsi per i dati eliminati
- Se un elemento è stato eliminato con successo
- L'ora in cui un elemento è stato eliminato

Esempi di report sulle attività

Il livello di dettaglio del rapporto sulle attività dipende da te. Ecco alcuni esempi di report di dati trasferiti con la seguente configurazione:

- Tipo di rapporto: standard
- Livello di rapporto: successi ed errori

> **Note**
>
> I report utilizzano lo standard ISO-8601 per il formato del timestamp. I tempi sono espressi in UTC e misurati in nanosecondi. Questo comportamento è diverso dal modo in cui vengono misurate altre metriche dei report sulle attività. Ad esempio, i dettagli sull'esecuzione delle attività, come `TransferDuration` `eVerifyDuration`, vengono misurati in millisecondi.

I report sulle attività in modalità avanzata utilizzano uno schema leggermente diverso rispetto ai report sulle attività in modalità base. Gli esempi seguenti possono aiutarti a sapere cosa aspettarti dai tuoi report a seconda della modalità di attività utilizzata.

Esempi di report sui dati trasferiti con stato di successo

I seguenti report mostrano i trasferimenti riusciti per un oggetto denominato`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": "jtqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
        "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"
    }]
}
```

Esempi di report sui dati trasferiti con stato di errore

I seguenti report forniscono esempi di quando non è DataSync possibile trasferire un oggetto denominato`object1.txt`.

Enhanced mode

Questo rapporto mostra che non è DataSync possibile accedere a un oggetto denominato a `object1.txt` causa di un problema di AWS KMS autorizzazioni. (Se ricevi un errore come questo, consultaAccesso ai bucket S3 utilizzando la crittografia lato server.)

```
{
    "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

Questo rapporto mostra che un oggetto denominato `object1.txt` non è stato trasferito a causa di un problema di autorizzazioni del bucket S3. (Se ricevi un errore come questo, vedi.) [Fornire DataSync l'accesso ai bucket S3]

```
{
    "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": "FAILED",
        "FailureReason": "S3 Get Object Failed",
        "FailureCode": 40974
    }]
}
```

Limitazioni

- I report sulle attività individuali non possono superare i 5 MB. Se stai copiando un numero elevato di file, il rapporto sulle attività potrebbe essere suddiviso in più report.
- Esistono situazioni in cui la creazione di report sulle attività può influire sulle prestazioni del trasferimento dei dati. Ad esempio, potresti notarlo quando la tua connessione di rete ha un'elevata latenza e i file che stai trasferendo sono piccoli o stai copiando solo le modifiche dei metadati.

Creazione dei report sulle attività DataSync

AWS DataSync i report sulle attività possono essere solo un riepilogo dell'esecuzione dell'attività o una serie di report dettagliati su quali DataSync tentativi di trasferire, ignorare, verificare ed eliminare.

Prerequisiti

Prima di poter creare un rapporto sulle attività, è necessario effettuare le seguenti operazioni.

Argomenti

- Crea un bucket S3 per i tuoi report sulle attività
- Consenti DataSync di caricare report sulle attività nel tuo bucket S3

Crea un bucket S3 per i tuoi report sulle attività

Se non ne hai già uno, crea un bucket S3 in cui caricare il tuo rapporto sulle DataSync attività. I report vengono archiviati nella classe di storage S3 Standard.

Per questo bucket consigliamo quanto segue:

- Se hai intenzione di trasferire dati in un bucket S3, non utilizzare lo stesso bucket per il report delle attività se disabiliti l'opzione Mantieni i file eliminati. Altrimenti, DataSync eliminerà tutti i report sulle attività precedenti ogni volta che esegui un'attività, poiché tali report non esistono nella posizione di origine.
- Per evitare una configurazione complessa delle autorizzazioni di accesso, assicurati che il bucket dei report sulle attività si trovi nella stessa Account AWS area geografica dell'attività di DataSync trasferimento.

Consenti DataSync di caricare report sulle attività nel tuo bucket S3

Devi configurare un ruolo AWS Identity and Access Management (IAM) che DataSync consenta di caricare un report sulle attività nel tuo bucket S3.

Nella DataSync console, puoi creare un ruolo IAM che nella maggior parte dei casi include automaticamente le autorizzazioni per caricare un report di attività nel tuo bucket. Tieni presente che questo ruolo generato automaticamente potrebbe non soddisfare le tue esigenze dal punto di vista del privilegio minimo. Inoltre, questo ruolo non funzionerà se il bucket è crittografato con una chiave gestita dal cliente AWS Key Management Service () (AWS KMS SSE-KMS). In questi casi, puoi creare il ruolo manualmente purché il ruolo esegua almeno le seguenti operazioni:

- Evita il problema del vicedirettore confuso tra servizi nell'entità fidata del ruolo.

  L'esempio completo seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition per evitare il problema del confuso vice con DataSync.

  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:*"
                }
            }
        }
    ]
}
```

- Consente di DataSync caricare un report sulle attività nel bucket S3.

L'esempio seguente esegue questa operazione includendo l'`s3:PutObject`azione solo per un prefisso specifico (`reports/`) nel bucket.

JSON

```
{
        "Version": "2012-10-17",
        "Statement": [{
            "Action": [
                "s3:PutObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::your-task-reports-bucket/reports/*"
        }]
}
```

- Se il bucket S3 è crittografato con una chiave SSE-KMS gestita dal cliente, la policy della chiave deve includere il ruolo IAM utilizzato per accedere al bucket. DataSync

  Per ulteriori informazioni, consulta Accesso ai bucket S3 utilizzando la crittografia lato server.

Creazione di un rapporto di attività di solo riepilogo

È possibile configurare un rapporto sulle attività che includa un riepilogo solo al DataSync momento della creazione, dell'avvio dell'attività o dell'aggiornamento dell'attività.

I passaggi seguenti mostrano come configurare un rapporto di attività di solo riepilogo durante la creazione di un'attività.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Scorri verso il basso fino alla sezione Rapporto sulle attività. Per Tipo di rapporto, scegli Solo riepilogo.

5. Per il bucket S3 per i report, scegli un bucket S3 in cui DataSync caricare il rapporto sulle attività.

   > **Tip**
   >
   > Se hai intenzione di trasferire dati in un bucket S3, non utilizzare lo stesso bucket per il report delle attività se disabiliti l'opzione Mantieni i file eliminati. Altrimenti, DataSync eliminerà tutti i report sulle attività precedenti ogni volta che esegui un'attività, poiché tali report non esistono nella posizione di origine.

6. Per Cartella, inserisci un prefisso da utilizzare per il rapporto sulle attività quando DataSync carichi il rapporto nel tuo bucket S3 (ad esempio,). **`reports/`**

   Assicurati di includere il carattere delimitatore appropriato alla fine del prefisso. Questo carattere è in genere una barra (). / Per ulteriori informazioni, consulta Organization object using prefixes nella Amazon S3 User Guide.

7. In IAM role (Ruolo IAM), eseguire una delle seguenti operazioni:

   - Scegli Autogenerate per creare DataSync automaticamente un ruolo IAM con le autorizzazioni necessarie per accedere al bucket S3.

     Se DataSync in precedenza hai creato un ruolo IAM per questo bucket S3, quel ruolo viene scelto per impostazione predefinita.
   - Scegli un ruolo IAM personalizzato che hai creato.

     In alcuni casi, potresti dover creare il ruolo da solo. Per ulteriori informazioni, consulta Consenti DataSync di caricare report sulle attività nel tuo bucket S3.

     > **Important**
     >
     > Se il bucket S3 è crittografato con una chiave SSE-KMS gestita dal cliente, la policy della chiave deve includere il ruolo IAM DataSync utilizzato per accedere al bucket. Per ulteriori informazioni, consulta Accesso ai bucket S3 utilizzando la crittografia lato server.

8. Completa la creazione dell'attività, quindi avvia l'attività per iniziare a trasferire i dati.

Una volta completato il trasferimento, puoi visualizzare il rapporto sull'attività.

Utilizzando il AWS CLI

1. Copiate il seguente comando `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. Per il `--source-location-arn` parametro, specifica l'Amazon Resource Name (ARN) della posizione di origine nel trasferimento. Sostituiscilo *us-east-1* con l'ID appropriato Regione AWS, sostituiscilo *123456789012* con il Account AWS numero appropriato e sostituiscilo *12345678abcdefgh* con l'ID della posizione di origine appropriato.
3. Per il `--destination-location-arn` parametro, specifica l'ARN della località di destinazione nel trasferimento. Sostituisci *us-east-1* con l'appropriato Regione AWS, sostituisci *123456789012* con il Account AWS numero appropriato e sostituisci *abcdefgh12345678* con l'ID della località di destinazione appropriato.
4. Per il `--task-report-config` parametro, effettuate le seguenti operazioni:

   - `Subdirectory`— Sostituisci *reports/* con il prefisso nel tuo bucket S3 il punto in cui desideri DataSync caricare i report delle attività.

     Assicurati di includere il carattere delimitatore appropriato alla fine del prefisso. Questo carattere è in genere una barra (). `/` Per ulteriori informazioni, consulta Organization object using prefixes nella Amazon S3 User Guide.
   - `S3BucketArn`— Specificare l'ARN del bucket S3 in cui si desidera caricare il report delle attività.

> **Tip**
>
> Se hai intenzione di trasferire dati in un bucket S3, non utilizzare lo stesso bucket per il report delle attività se disabiliti l'opzione Mantieni i file eliminati. Altrimenti, DataSync eliminerà tutti i report sulle attività precedenti ogni volta che esegui un'attività, poiché tali report non esistono nella posizione di origine.

- `BucketAccessRoleArn`— Specificate il ruolo IAM che DataSync consente di caricare un report di attività nel bucket S3.

  Per ulteriori informazioni, consulta Consenti DataSync di caricare report sulle attività nel tuo bucket S3.

  > **Important**
  >
  > Se il bucket S3 è crittografato con una chiave SSE-KMS gestita dal cliente, la policy della chiave deve includere il ruolo IAM utilizzato per accedere al bucket. DataSync Per ulteriori informazioni, consulta Accesso ai bucket S3 utilizzando la crittografia lato server.

- `OutputTypeSUMMARY_ONLY`— Specificare.

  Per ulteriori informazioni, consulta Riepilogano solo i rapporti sulle attività.

5. Esegui il `create-task` comando per creare l'attività.

   Riceverai una risposta come la seguente che ti mostra l'ARN dell'attività che hai creato. Avrai bisogno di questo ARN per eseguire il `start-task-execution` comando.

   ```
   {
       "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
   }
   ```

6. Copia il seguente `start-task-execution` comando.

   ```
   aws datasync-task-report start-task-execution \
     --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
   ```

7. Per il `--task-arn` parametro, specifica l'ARN dell'attività che stai avviando. Usa l'ARN che hai ricevuto dall'esecuzione del `create-task` comando.

8. Esegui il comando `start-task-execution`.

Una volta completato il trasferimento, puoi visualizzare il rapporto sulle attività.

Creazione di un rapporto sulle attività standard

È possibile configurare un rapporto di attività standard quando si crea DataSync un'attività, si avvia un'attività o si aggiorna l'attività.

I passaggi seguenti mostrano come configurare un report di attività standard durante la creazione di un'attività.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Scorri verso il basso fino alla sezione Rapporto sulle attività. Per Tipo di rapporto, scegli Rapporto standard.
5. Per Livello di rapporto, scegli una delle seguenti opzioni:

   - Solo errori: il rapporto sulle attività include solo i problemi relativi a ciò che DataSync hai cercato di trasferire, ignorare, verificare ed eliminare.
   - Successi ed errori: il rapporto sulle attività include gli elementi trasferiti, saltati, verificati ed eliminati DataSync con successo e quelli che non sono stati trasferiti.
   - Personalizzato: consente di scegliere se visualizzare solo gli errori o i successi e gli errori per aspetti specifici del rapporto sulle attività.

     Ad esempio, puoi scegliere Successi ed errori per l'elenco dei file trasferiti, ma Errori solo per il resto del rapporto.
6. Se stai effettuando il trasferimento in un bucket S3 che utilizza il controllo delle versioni degli oggetti, mantieni selezionata l'opzione Includi le versioni degli oggetti di Amazon S3 se desideri che il report includa la nuova versione per ogni oggetto trasferito.
7. Per il bucket S3 per i report, scegli un bucket S3 in cui caricare il report delle attività. DataSync

> **Tip**
>
> Se hai intenzione di trasferire dati in un bucket S3, non utilizzare lo stesso bucket per il report delle attività se disabiliti l'opzione Mantieni i file eliminati. Altrimenti, DataSync eliminerà tutti i report sulle attività precedenti ogni volta che esegui un'attività, poiché tali report non esistono nella posizione di origine.

8. Per Cartella, inserisci un prefisso da utilizzare per il rapporto sulle attività quando DataSync carichi il rapporto nel tuo bucket S3 (ad esempio,). **`reports/`** Assicurati di includere il carattere delimitatore appropriato alla fine del prefisso. Questo carattere è in genere una barra (). `/` Per ulteriori informazioni, consulta Organization object using prefixes nella Amazon S3 User Guide.
9. In IAM role (Ruolo IAM), eseguire una delle seguenti operazioni:
   - Scegli Autogenerate per creare DataSync automaticamente un ruolo IAM con le autorizzazioni necessarie per accedere al bucket S3.

     Se DataSync in precedenza hai creato un ruolo IAM per questo bucket S3, quel ruolo viene scelto per impostazione predefinita.
   - Scegli un ruolo IAM personalizzato che hai creato.

     In alcuni casi, potresti dover creare il ruolo da solo. Per ulteriori informazioni, consulta Consenti DataSync di caricare report sulle attività nel tuo bucket S3.

     > **Important**
     >
     > Se il bucket S3 è crittografato con una chiave SSE-KMS gestita dal cliente, la policy della chiave deve includere il ruolo IAM DataSync utilizzato per accedere al bucket. Per ulteriori informazioni, consulta Accesso ai bucket S3 utilizzando la crittografia lato server.
10. Completa la creazione dell'attività e avvia l'attività per iniziare a trasferire i dati.

Una volta completato il trasferimento, puoi visualizzare il rapporto sull'attività.

Utilizzando il AWS CLI

1. Copia il seguente `create-task` comando:

```
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. Per il `--source-location-arn` parametro, specificate l'ARN della posizione di origine nel trasferimento. Sostituisci *us-east-1* con l'appropriato Regione AWS, sostituisci *123456789012* con il Account AWS numero appropriato e sostituisci *12345678abcdefgh* con l'ID della posizione di origine appropriato.
3. Per il `--destination-location-arn` parametro, specifica l'ARN della località di destinazione nel trasferimento. Sostituisci *us-east-1* con l'appropriato Regione AWS, sostituisci *123456789012* con il Account AWS numero appropriato e sostituisci *abcdefgh12345678* con l'ID della località di destinazione appropriato.
4. Per il `--task-report-config` parametro, effettuate le seguenti operazioni:

   - `Subdirectory`— Sostituisci *reports/* con il prefisso nel tuo bucket S3 il punto in cui desideri DataSync caricare i report delle attività. Assicurati di includere il carattere delimitatore appropriato alla fine del prefisso. Questo carattere è in genere una barra (). `/` Per ulteriori informazioni, consulta Organization object using prefixes nella Amazon S3 User Guide.
   - `S3BucketArn`— Specificare l'ARN del bucket S3 in cui si desidera caricare il report delle attività.

     > **Tip**
     >
     > Se hai intenzione di trasferire dati in un bucket S3, non utilizzare lo stesso bucket per il report delle attività se disabiliti l'opzione Mantieni i file eliminati. Altrimenti, DataSync

eliminerà tutti i report sulle attività precedenti ogni volta che esegui un'attività, poiché tali report non esistono nella posizione di origine.

- `BucketAccessRoleArn`— Specificate il ruolo IAM che DataSync consente di caricare un report di attività nel bucket S3.

  Per ulteriori informazioni, consulta Consenti DataSync di caricare report sulle attività nel tuo bucket S3.

  > **Important**
  >
  > Se il bucket S3 è crittografato con una chiave SSE-KMS gestita dal cliente, la policy della chiave deve includere il ruolo IAM utilizzato per accedere al bucket. DataSync Per ulteriori informazioni, consulta Accesso ai bucket S3 utilizzando la crittografia lato server.

- `OutputTypeSTANDARD`— Specificare il rapporto.

  Per ulteriori informazioni, vedere Rapporti sulle attività standard Tipi di report sulle attività.

- (Facoltativo)`ReportLevel`: specifica se desideri `ERRORS_ONLY` (impostazione predefinita) o `SUCCESSES_AND_ERRORS` nel rapporto.
- (Facoltativo)`ObjectVersionIds`: se stai effettuando il trasferimento in un bucket S3 che utilizza il controllo delle versioni degli oggetti, specifica `NONE` se non desideri includere la nuova versione per ogni oggetto trasferito nel rapporto.

  Per impostazione predefinita, questa opzione è impostata su. `INCLUDE`

- (Facoltativo)`Overrides`: personalizza un aspetto particolare del rapporto. `ReportLevel`

  Ad esempio, potresti voler visualizzare `SUCCESSES_AND_ERRORS` l'elenco degli elementi DataSync eliminati nella località di destinazione, ma desideri visualizzare tutto `ERRORS_ONLY` il resto. In questo esempio, aggiungeresti la seguente `Overrides` opzione al `--task-report-config` parametro:

```
"Overrides":{
  "Deleted":{
    "ReportLevel":"SUCCESSES_AND_ERRORS"
  }
}
```

Se non lo usi`Overrides`, l'intero rapporto utilizza quello `ReportLevel` che hai specificato.

5. Esegui il `create-task` comando per creare l'attività.

   Riceverai una risposta come la seguente che ti mostra l'ARN dell'attività che hai creato. Avrai bisogno di questo ARN per eseguire il `start-task-execution` comando.

   ```
   {
       "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
   }
   ```

6. Copia il seguente `start-task-execution` comando.

   ```
   aws datasync-task-report start-task-execution \
     --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
   ```

7. Per il `--task-arn` parametro, specifica l'ARN dell'attività che stai eseguendo. Usa l'ARN che hai ricevuto dall'esecuzione del `create-task` comando.
8. Esegui il comando `start-task-execution`.

Una volta completato il trasferimento, puoi visualizzare il rapporto sulle attività.

Visualizzazione dei report sulle DataSync attività

DataSync crea report sulle attività per ogni esecuzione di attività. Una volta completata l'esecuzione, puoi trovare i relativi report sulle attività nel tuo bucket S3. I report sulle attività sono organizzati in base a prefissi che includono le attività e le relative IDs esecuzioni.

Per aiutarti a localizzare i report sulle attività nel tuo bucket S3, usa questi esempi:

- Rapporto sulle attività, solo riepilogativo: *`reports-prefix`*`/Summary-Reports/`*`task-id-folder`*`/`*`task-execution-id-folder`*
- Rapporto sulle attività standard — *`reports-prefix`*`/Detailed-Reports/`*`task-id-folder`*`/`*`task-execution-id-folder`*

Poiché i report sulle attività sono in formato JSON, sono disponibili diverse opzioni per visualizzarli:

- Visualizza un report utilizzando Amazon S3 Select.

- Visualizza i report utilizzando AWS servizi come AWS Glue Amazon Athena e Amazon. QuickSight Per ulteriori informazioni sulla visualizzazione dei report sulle attività, consulta lo Storage Blog.AWS

Monitoraggio dei trasferimenti di dati con Amazon CloudWatch Logs

È possibile monitorare il AWS DataSync trasferimento utilizzando CloudWatch Logs. Si consiglia di configurare l'attività in modo da registrare almeno le informazioni di base (come gli errori di trasferimento).

Consentire DataSync il caricamento dei log in un gruppo di CloudWatch log

Per configurare la registrazione per l' DataSyncattività, è necessario un gruppo di CloudWatch log a cui DataSync sia consentito inviare i log. È possibile configurare questo accesso tramite un ruolo AWS Identity and Access Management (IAM). Il modo in cui funziona in modo specifico dipende dalla modalità di attività.

Enhanced mode

Con la modalità avanzata, invia DataSync automaticamente i registri delle attività a un gruppo di log denominato`/aws/datasync`. Se quel gruppo di log non esiste nel tuo Regione AWS, DataSync crea il gruppo di log per tuo conto utilizzando un ruolo collegato ai servizi IAM quando crei l'attività.

Basic mode

Esistono due modi per configurare un gruppo di CloudWatch log per un' DataSync attività utilizzando la modalità Basic. Nella console, puoi creare automaticamente un ruolo IAM che nella maggior parte dei casi include le autorizzazioni DataSync necessarie per caricare i log. Tieni presente che questo ruolo generato automaticamente potrebbe non soddisfare le tue esigenze dal punto di vista del privilegio minimo.

Se desideri utilizzare un gruppo di CloudWatch log esistente o stai creando le tue attività a livello di codice, devi creare tu stesso il ruolo IAM.

L'esempio seguente è una policy IAM che concede queste autorizzazioni.

```
{
```

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

La policy utilizza `Condition` istruzioni per garantire che solo DataSync le attività dell'account specificato abbiano accesso al gruppo di CloudWatch log specificato. Si consiglia di utilizzare le chiavi di contesto aws:SourceArne aws:SourceAccountglobal condition in queste `Condition` istruzioni per evitare il confuso problema del vice. Per ulteriori informazioni, consulta Prevenzione del problema "confused deputy" tra servizi.

Per specificare l' DataSync attività o le attività, sostituiscile *`region`* con il codice regionale del Regione AWS luogo in cui si trovano le attività (ad esempio,`us-west-2`) e sostituiscilo *`account-id`* con l' Account AWS ID dell'account che contiene le attività. Per specificare il gruppo di CloudWatch log, sostituisci gli stessi valori. È inoltre possibile modificare l'`Resource`istruzione per indirizzarla a gruppi di log specifici. Per ulteriori informazioni sull'utilizzo di `SourceArn` and`SourceAccount`, consulta la sezione Global condition keys nella IAM User Guide.

Per applicare la policy, salvare questa istruzione di policy in un file nel computer locale. Quindi esegui il AWS CLI comando seguente per applicare la politica delle risorse. Per utilizzare questo comando di esempio, sostituiscilo *`full-path-to-policy-file`* con il percorso del file che contiene la dichiarazione sulla politica.

```
aws logs put-resource-policy --policy-name trust-datasync --policy-document
 file://full-path-to-policy-file
```

> **Note**
>
> Esegui questo comando utilizzando lo stesso comando Account AWS e Regione AWS dove hai attivato il tuo DataSync agente.

Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.

Configurazione della registrazione per la tua attività DataSync

Ti consigliamo di configurare almeno un certo livello di registrazione per la tua attività. DataSync

Prima di iniziare

DataSync necessita dell'autorizzazione per caricare i log in un gruppo di CloudWatch log. Per ulteriori informazioni, consulta Consentire DataSync il caricamento dei log in un gruppo di CloudWatch log.

Utilizzo della console di DataSync

Le seguenti istruzioni descrivono come configurare la CloudWatch registrazione durante la creazione di un'attività. È inoltre possibile configurare la registrazione quando si modifica un'attività.

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività e quindi scegli Crea attività.
3. Configura le posizioni di origine e di destinazione dell'attività.

   Per ulteriori informazioni, consulta Con chi posso trasferire i miei dati AWS DataSync?
4. Nella pagina Configura impostazioni, scegli una modalità di attività e qualsiasi altra opzione.

   Potrebbero interessarti alcune delle seguenti opzioni:

- Specificate quali dati trasferire utilizzando un manifesto o dei filtri.
- Configura come gestire i metadati dei file e verificare l'integrità dei dati.

5. Per Livello di registro, scegli una delle seguenti opzioni:

   - Registra informazioni di base come gli errori di trasferimento: pubblica i log con solo informazioni di base (come gli errori di trasferimento).
   - Registra tutti gli oggetti e i file trasferiti: pubblica i registri di tutti i file o oggetti che DataSync trasferisce ed esegue controlli di integrità dei dati.
   - Non generare registri

6. Effettua una delle seguenti operazioni a seconda della modalità di attività che stai utilizzando per creare o specificare un gruppo di CloudWatch log:

   Enhanced mode

   Quando scegli Crea attività, utilizza (o crea) DataSync automaticamente un gruppo di log denominato`/aws/datasync`.

   Basic mode

   Per CloudWatch il gruppo di log, specifica un gruppo di log su cui DataSync è consentito caricare i log effettuando una delle seguenti operazioni:

   - Scegliete Generazione automatica per creare automaticamente un gruppo di log che DataSync consenta di caricarvi i log.
   - Scegli un gruppo di log esistente nel tuo attuale. Regione AWS

     Se scegli un gruppo di log esistente, assicurati che DataSync sia autorizzato a caricare i log in quel gruppo di log.

7. Scegli Create task (Crea attività).

Sei pronto per iniziare la tua attività.

Usando il AWS CLI

1. Copia il seguente `create-task` comando:

```
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. Per`--source-location-arn`, specifica l'Amazon Resource Name (ARN) della tua posizione di origine.
3. Per`--destination-location-arn`, specifica l'ARN della località di destinazione.

   Se effettui trasferimenti tra Regioni AWS i nostri account, assicurati che l'ARN includa l'altra regione o l'ID dell'account.
4. Per`--task-mode`, specifica `ENHANCED` o. `BASIC`
5. (Consigliato) Per`--name`, specificate un nome per l'attività che possiate ricordare.
6. Per`LogLevel`, specifica una delle seguenti opzioni:

   - `BASIC`— Pubblica registri con solo informazioni di base (come errori di trasferimento).
   - `TRANSFER`— Pubblica i registri per tutti i file o gli oggetti che DataSync trasferiscono ed eseguono controlli di integrità dei dati.
   - `NONE`— Non generare registri.
7. Per `--cloudwatch-log-group-arn`, specifica l'ARN di un gruppo di CloudWatch log.

   > **Important**
   >
   > Se il tuo `--task-mode` è`ENHANCED`, non è necessario specificare questa opzione. Per ulteriori informazioni, consulta Consentire DataSync il caricamento dei log in un gruppo di CloudWatch log.
8. Esegui il comando `create-task`.

   Se il comando ha esito positivo, si ottiene una risposta che mostra l'ARN dell'attività creata. Per esempio:

```
{
```

```
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Sei pronto per iniziare la tua attività.

Utilizzando l' DataSync API

È possibile configurare CloudWatch la registrazione per l'attività utilizzando il `CloudWatchLogGroupArn` parametro con una delle seguenti operazioni:

- CreateTask
- UpdateTask

Visualizzazione dei registri delle DataSync attività

All'avvio dell'attività, è possibile visualizzare i registri di esecuzione dell'attività utilizzando la CloudWatch console o AWS CLI (tra le altre opzioni). Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.

DataSync fornisce log strutturati in JSON per attività in modalità avanzata. Le attività in modalità base hanno registri non strutturati. Gli esempi seguenti mostrano come vengono visualizzati gli errori di verifica nei log in modalità Avanzata rispetto ai log in modalità Basic.

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 extAttrsHash=0
[NOTICE]   dstHash: f9c2cca900301d38b0930367d8d587153154af467da0fdcf1bebc0848ec72c0d
```

Registrazione delle chiamate AWS DataSync API con AWS CloudTrail

AWS DataSync è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un membro Servizio AWS . DataSync CloudTrail acquisisce tutte le chiamate API DataSync come eventi. Le chiamate acquisite includono chiamate dalla DataSync console e chiamate di codice alle operazioni DataSync API.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS DataSync Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS DataSync, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Utilizzo delle DataSync informazioni in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in AWS DataSync, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella Cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nell' Account AWS che includa gli eventi per AWS DataSync, crea un trail. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi da tutti Regioni AWS nella stessa AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte DataSync le azioni vengono registrate da CloudTrail. (Per ulteriori informazioni, consulta il riferimento all' DataSync API.)

Ad esempio, le chiamate alle `ListLocations` operazioni `CreateAgentCreateTask`, e generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, consulta CloudTrail userIdentity elemento nella Guida per l'AWS CloudTrail utente.

Comprendere DataSync le voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`CreateTask`operazione.

```
{
    "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"
}
```


Monitoraggio degli eventi tramite Amazon EventBridge

EventBridge Gli eventi Amazon descrivono i cambiamenti nelle DataSync risorse. Puoi configurare regole corrispondenti a questi eventi e instradarli verso una o più funzioni o flussi target. Gli eventi vengono emessi sulla base del best effort.

DataSync eventi di trasferimento

I seguenti EventBridge eventi sono disponibili per DataSync i trasferimenti.

Agent state changes

Evento	Descrizione

Agent state changes

Online	L'agente è configurato correttamente e pronto all'uso. Questo è lo stato di funzionamento normale di un agente.
Offline	L'agente non è in contatto con il DataSync servizio da almeno cinque minuti. Questo può succedere per diversi motivi. Per ulteriori informazioni, consulta Cosa devo fare se il mio agente è offline?

Location state changes

Evento	Descrizione
Aggiungendo	DataSync sta aggiungendo una posizione.
Disponibilità	La posizione è stata creata ed è disponibile per l'uso.

Task state changes

Evento	Descrizione
Disponibilità	L'attività è stata creata ed è pronta per essere avviata.
In esecuzione	L'operazione è in corso e funziona correttam ente.
Non disponibile	L'attività non è configurata correttamente e non può essere utilizzata. Potresti vedere questo evento quando un agente associato all'attività va offline.
Accodati	Un'altra attività è in esecuzione e utilizza lo stesso agente. DataSync esegue le attività in serie (first in, first out).

Agent state changes

Task execution state changes

Evento	Descrizione
In coda	L'esecuzione di un'altra attività è in esecuzione e utilizza lo stesso DataSync agente. Per ulteriori informazioni, consulta Sapere quando l'attività è in coda.
Avvio	DataSync sta inizializzando l'esecuzione dell'attività. Questo stato in genere passa rapidamente, ma può richiedere fino a qualche minuto.
Preparing (Preparazione)	DataSync sta determinando quali dati trasferire. Questo passaggio può richiedere alcuni minuti o alcune ore a seconda del numero di file, oggetti o directory in entrambe le posizioni e della configurazione dell'attività. Inoltre, la preparazione potrebbe non essere applicabile all'attività. Per ulteriori informazioni, consulta Come si DataSync prepara il trasferimento dei dati.
Trasferimento	DataSync sta effettuando il trasferimento effettivo dei dati.
Verifica in corso	DataSync sta eseguendo un controllo dell'integrità dei dati al termine del trasferimento.
Riuscito	L'esecuzione dell'operazione è riuscita.
Annullamento in corso	L'esecuzione dell'attività è in fase di annullamento.
Errore	L'esecuzione dell'operazione non è riuscita.

Monitoraggio AWS DataSync con strumenti manuali

Puoi tenere traccia dei tuoi AWS DataSync trasferimenti dalla console o dalla riga di comando.

Monitoraggio del trasferimento tramite la DataSync console

Puoi monitorare il DataSync trasferimento utilizzando la console, che fornisce metriche in tempo reale come il trasferimento dei dati, la velocità effettiva di dati e file e la compressione dei dati.

Per monitorare il trasferimento utilizzando la console DataSync

1. Dopo aver avviato l' DataSync attività, scegli Visualizza i dettagli di esecuzione.
2. Visualizza le metriche relative al trasferimento.

Monitoraggio del trasferimento utilizzando il AWS CLI

È possibile monitorare il DataSync trasferimento utilizzando AWS Command Line Interface (AWS CLI).

Copia il seguente `describe-task-execution` comando. Per utilizzare questo comando di esempio, sostituisci *`user input placeholders`* con le tue informazioni.

```
aws datasync describe-task-execution \
  --task-execution-arn 'arn:aws:datasync:region:account-id:task/task-id/execution/task-execution-id'
```

Questo comando restituisce informazioni sull'esecuzione di un'attività simili a quelle mostrate di seguito.

```
{
    "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-
aaaabbbbccccddddf/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": "SUCCESSES_AND_ERRORS"
            },
            "Transferred": {
```

```
                "ReportLevel": "ERRORS_ONLY"
            },
            "Verified": {
                "ReportLevel": "ERRORS_ONLY"
            }
        },
        "ReportLevel": "ERRORS_ONLY"
    }
}
```

- Se l'esecuzione dell'attività riesce, il valore di Status (Stato) cambia in SUCCESS (RIUSCITO). Per informazioni sul significato degli elementi di risposta, vedereDescribeTaskExecution.
- Se l'esecuzione dell'attività non riesce, il risultato invia codici di errore che possono aiutarti a risolvere i problemi. Per informazioni sui codici di errore, vedere. TaskExecutionResultDetail

Monitoraggio del trasferimento tramite l'**`watch`**utilità

Per monitorare lo stato di avanzamento dell'attività in tempo reale dalla riga di comando, è possibile utilizzare l'`watch`utilità Unix standard. I valori della durata dell'esecuzione dell'attività vengono misurati in millisecondi.

L'`watch`utilità non riconosce l'alias. DataSync L'esempio seguente mostra come richiamare direttamente la CLI. Per utilizzare questo comando di esempio, sostituisci *`user input placeholders`* con le tue informazioni.

```
# 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'"
```

Gestione delle AWS DataSync risorse

Scopri come gestire AWS DataSync le tue risorse, come agenti, sedi e attività.

Gestire il tuo DataSync agente

Una volta attivato un DataSync agente, lo AWS gestisce al posto tuo (inclusi gli aggiornamenti software). Ulteriori informazioni

Verifica della connettività e delle risorse di sistema del tuo DataSync agente

Sebbene AWS gestisca DataSync l'agente una volta distribuito e attivato, in alcuni casi potrebbe essere necessario modificare le impostazioni dell'agente o risolvere un problema. Ulteriori informazioni

Sostituzione del tuo agente DataSync

Per sostituire un DataSync agente, è necessario creare un nuovo agente e aggiornare tutte le sedi che utilizzano il vecchio agente. Ulteriori informazioni

Pulizia DataSync delle risorse

Se le hai utilizzate DataSync per un test o semplicemente non ti servono più le sue risorse, elimina quelle risorse in modo che non ti vengano addebitate spese. Ulteriori informazioni

Riutilizzo dell'infrastruttura di un DataSync agente

Dopo aver eliminato una risorsa agente da DataSync, puoi comunque utilizzare la macchina virtuale o l' EC2 istanza Amazon dell'agente per attivare un nuovo agente. Ulteriori informazioni

Gestire il tuo AWS DataSync agente

Una volta attivato un AWS DataSync agente, AWS gestisce l'appliance della macchina virtuale (VM) per te.

Aggiornamenti del software dell'agente

AWS aggiorna automaticamente il software dell'agente, incluso il sistema operativo sottostante e i relativi pacchetti DataSync software.

DataSync aggiorna l'agente solo quando è inattivo. Ad esempio, il tuo agente non verrà aggiornato fino al completamento del trasferimento.

L'agente potrebbe andare offline per un breve periodo dopo gli aggiornamenti. Ciò può accadere, ad esempio, poco dopo l'attivazione dell'agente quando AWS aggiorna l'agente.

Important

- DataSync applica automaticamente e regolarmente le patch agli agenti per mantenerne la sicurezza e la stabilità. DataSync gli agenti utilizzano Amazon Linux 2 come sistema operativo di base. Puoi visualizzare lo stato attuale dei problemi CVE (Common Vulnerabilities and Exposures) rilevati su Amazon Linux Security Center. Le patch CVE vengono applicate automaticamente entro 30 giorni dalla data di rilascio, come indicato su Amazon Linux Security Center. L'applicazione delle patch avviene finché l'agente è online e non esegue attivamente l'esecuzione di un'attività.
- DataSync non supporta l'aggiornamento manuale di un EC2 agente Amazon con direttive cloud-init. Se aggiorni un agente in questo modo, potresti riscontrare problemi di interoperabilità per DataSync cui non puoi attivare o utilizzare l'agente.

Stati degli agenti

La tabella seguente descrive lo stato degli DataSync agenti.

Stato agente	Significato
Online	L'agente è configurato correttamente e pronto all'uso. Questo è lo stato di funzionamento normale di un agente.
Offline	L'agente non è in contatto con il DataSync servizio da cinque minuti o più. Questo può succedere per

Stato agente	Significato
	diversi motivi. Per ulteriori informazioni, consulta Cosa devo fare se il mio agente è offline?

Risoluzione dei problemi relativi al tuo agente

Sebbene AWS gestisca l' DataSync agente al posto tuo, in alcuni casi potresti dover lavorare nuovamente direttamente con lui. Ad esempio, se l'agente va offline o perde la connessione al sistema di storage locale, puoi provare a risolvere questi problemi nella console locale dell'agente.

Per ulteriori informazioni, consulta la sezione relativa alla risoluzione dei problemi DataSync degli agenti.

Esecuzione della manutenzione sul tuo agente

Sebbene AWS gestisca AWS DataSync l'agente una volta distribuito e attivato, in alcuni casi potrebbe essere necessario modificare le impostazioni dell'agente o risolvere un problema. Ecco alcuni esempi dei motivi per cui dovresti lavorare con il tuo agente tramite la sua console locale:

- Assegna manualmente un indirizzo IP all'agente.
- Controlla le risorse di sistema del tuo agente.

> **Important**
>
> Non è necessario utilizzare la console locale dell'agente per le DataSync funzionalità standard.

Accesso alla console locale dell'agente

Il modo in cui accedi alla console locale dipende dal tipo di agente che stai utilizzando.

Accesso alla console locale (VMware ESXiLinux KVM o Microsoft Hyper-V)

Per motivi di sicurezza, non è possibile connettersi in remoto alla console locale della macchina virtuale (VM) dell' DataSync agente.

- Se è la prima volta che utilizzi la console locale, accedi con le credenziali predefinite. Il nome utente predefinito è **`admin`** e la password è **`password`**. Ti verrà chiesto di cambiare la password al primo accesso.

  > **Note**
  >
  > Dopo la configurazione iniziale della password, puoi cambiarla in qualsiasi momento. Nel menu principale della console, inserisci il numero accanto a Prompt dei comandi, quindi esegui il `passwd` comando per modificare la password.

Accesso alla console locale (Amazon EC2)

Per connetterti alla console locale di un EC2 agente Amazon, devi usare SSH.

Prima di iniziare: assicurati che il gruppo di sicurezza dell' EC2 istanza consenta l'accesso con SSH (porta TCP 22).

1. Apri un terminale e copia il seguente comando: `ssh`

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

   - Per*`/path/key-pair-name`*, specifica il percorso e il nome del file (`.pem`) della chiave privata richiesta per connetterti all'istanza.
   - Per *`instance-user-name`*, specificare `admin`.
   - Per*`instance-public-ip-address`*, specifica l'indirizzo IP pubblico dell'istanza.
2. Esegui il `ssh` comando per connetterti all'istanza.

Una volta connesso, viene visualizzato il menu principale della console locale dell'agente.

Configurazione delle impostazioni DHCP, DNS e IP dell'agente

La configurazione di rete predefinita per l'agente è DHCP (Dynamic Host Configuration Protocol). Con DHCP, all'agente viene assegnato automaticamente un indirizzo IP. In alcuni casi, può essere necessario assegnare manualmente un indirizzo IP statico all'agente, come descritto di seguito.

1. Accedere alla console locale dell'agente.

2. Nel menu principale AWS DataSync Attivazione - Configurazione, accedi **1** per iniziare a configurare la rete.
3. Scegliere una delle seguenti opzioni dal menu Network Configuration (Configurazione di rete).

Per	Esegui questa operazione

Ottenere informazioni sulla scheda di rete	Specificare **1**.
	
	Viene visualizzato un elenco di nomi di adattatore e viene richiesto di immettere un nome di adattatore, ad esempio. **eth0** Se la scheda specificata è in uso, vengono visualizz ate le informazioni di rete relative a tale scheda, come nell'esempio seguente:
	
	`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:fd0`
	`0::4daf`
	`Prefix length: 128`
	`Gateway: fe80::5021:ff:ff88:4acd`
	`DHCPV6 enabled: Yes`
	
	`DNS: abcd:4444:e5ee:fd00::1`
	`DNS: 192.168.100.4`
	
	È possibile utilizzare lo stesso nome di scheda quando si configura un indirizzo IP statico (opzione 3) e quando si imposta la scheda di routing predefinita dell'agente (opzione 5).

Configurazione di DHCP	

Per	Esegui questa operazione
	Specificare **2**. Scegliete una versione IP da utilizzare, quindi configurate l'interfaccia di rete per utilizzare DHCP.
Come configurare un indirizzo IP statico per l'agente	Specificare **3**. Ti viene richiesto di scegliere il protocollo IP da utilizzare o IPv6 entrambi. IPv4 Quindi ti viene richiesto di inserire il nome dell'adattatore di rete per configurare un indirizzo IP statico. **Important** Se l'agente è già stato attivato, è necessario spegnerlo e riavviarlo dalla DataSync console affinché le impostazioni abbiano effetto.

Per	Esegui questa operazione
Reimpostare l'intera configurazione di rete dell'agente come DHCP	Specificare **4**. Scegli la versione IP da ripristinare su DHCP. Tutte le interfacce di rete per la versione IP scelta sono impostate per utilizzare DHCP. **Important** Se l'agente è già stato attivato, è necessario spegnerlo e riavviarlo dalla DataSync console affinché le impostazioni abbiano effetto.
Come impostare la scheda di routing predefinita dell'agente	Specificare **5**. Vengono visualizzati gli adattatori disponibili per l'agente e viene richiesto di scegliere uno degli adattatori, ad esempio. **`eth0`**
Modifica la configurazione DNS (Domain Name System) del tuo agente	Specificare **6**. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. Viene richiesto di fornire il nuovo indirizzo IP.

Per	Esegui questa operazione
Come visualizzare la configurazione DNS dell'agente	Specificare **7**. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. **Note** Per alcune versioni dell' VMware hypervisor, puoi modificare la configura zione dell'adattatore in questo menu.
Visualizzare le tabelle di routing	Specificare **8**. Scegliete la versione IP (IPv4o entrambe) per visualizzare la tabella di routing predefinita per il vostro agente. IPv6
Visualizza la versione IP del tuo agente per i trasferimenti di dati	Specificare **9**. L'impostazione della versione IP dell'agente per il trasferimento dei dati mostra `IPv4IPv6,IPv4 (auto)`, `oIPv6 (auto)`.
Modifica il protocollo IP del tuo agente per il trasferimento dei dati	Specificare **`10`**. Vengono visualizzate le impostazioni della versione IP disponibile per i trasferimenti di dati. È possibile scegliere tra `IPv4IPv6,IPv4 (auto)`, `oIPv6 (auto)`. Per ulteriori informazioni sull'impostazione della versione IP dell'agente per il trasferimento dei dati, consultathe section called “IPv6 supporto”.

Verifica delle risorse di sistema del tuo agente

Quando accedi alla console dell'agente, i core della CPU virtuale, le dimensioni del volume root e la RAM vengono controllati automaticamente. Se sono presenti errori o avvisi, questi vengono contrassegnati sul display del menu della console con un banner che fornisce dettagli su tali errori o avvisi.

Se non ci sono errori o avvisi all'avvio della console, il menu visualizza un testo bianco. Verrà visualizzata `(0 Errors)` l'opzione Visualizza controllo delle risorse di sistema.

Se sono presenti errori o avvisi, il menu della console visualizza il numero di errori e avvisi, rispettivamente in rosso e giallo, in un banner nella parte superiore del menu. Ad esempio, `(1 ERROR, 1 WARNING)`.

Per controllare le risorse di sistema del tuo agente

1. Accedere alla console locale dell'agente.
2. Nel menu principale AWS DataSync Attivazione - Configurazione, accedi **4** per visualizzare i risultati del controllo delle risorse di sistema.

   La console visualizza un messaggio [OK], [WARNING] ([ATTENZIONE]) o [FAIL] ([ESITO NEGATIVO]) per ogni risorsa, come descritto nella tabella seguente.

   Per EC2 le istanze Amazon, il controllo delle risorse di sistema verifica che il tipo di istanza sia una delle istanze consigliate per l'uso. DataSync Se il tipo di istanza corrisponde all'elenco, un singolo risultato viene visualizzato in verde, come segue.

   ```
   [ OK ] Instance Type Check
   ```

   Se l' EC2 istanza Amazon non è nell'elenco consigliato, il controllo delle risorse di sistema verifica le seguenti risorse.

   - Controllo dei core della CPU: sono necessari almeno quattro core.
   - Controllo della dimensione del disco: è richiesto un minimo di 80 GB di spazio disponibile su disco.
   - Controllo della RAM:
     - 32 GB di RAM assegnati all'istanza per l'esecuzione di attività con un massimo di 20 milioni di file, oggetti o directory.

- 64 GB di RAM assegnati all'istanza per l'esecuzione di attività con più di 20 milioni di file, oggetti o directory.
- Controllo dei flag della CPU: la CPU della VM dell'agente deve avere uno dei flag SSSE3 o SSE4 un set di istruzioni.

Se l' EC2 istanza Amazon non è nell'elenco delle istanze consigliate DataSync, ma dispone di risorse sufficienti, il risultato del controllo delle risorse di sistema mostra quattro risultati, tutti in verde.

Le stesse risorse vengono verificate per gli agenti distribuiti in Hyper-V, Linux Kernel-based Virtual Machine (KVM) e. VMware VMs

VMware agli agenti viene inoltre verificata la presenza di versioni supportate; le versioni non supportate causano un errore con banner rosso. Le versioni supportate includono VMware le versioni 6.5 e 6.7.

Sincronizzazione dell'ora sul tuo agente VMware

Se utilizzi un VMware agente, puoi visualizzare o modificare la configurazione del server NTP (Network Time Protocol) e sincronizzare l'ora dell'agente con l' VMware host dell'hypervisor.

1. Accedi alla console locale del tuo agente.
2. Nel menu principale AWS DataSync Attivazione - Configurazione, inserisci**5**.
3. Nel menu System Time Management, effettuate una delle seguenti operazioni:

Per	Esegui questa operazione
Visualizza e sincronizza l'ora della tua macchina virtuale con l'ora del server NTP	Specificare **1**. Viene visualizzata l'ora corrente del tuo agente. L'agente determina la differenza di fuso orario tra l'agente e il server NTP e richiede di sincronizzare gli orari. In alcune situazioni, l'orario di un agente potrebbe variare. Ad esempio, è possibile che

Per	Esegui questa operazione
	si verifichi un'interruzione prolungata della rete e che l'host e l'agente dell'hypervisor non ricevano aggiornamenti sull'ora, pertanto l'orario dell'agente è diverso da quello effettivo . Quando si verifica una deriva temporale come questa, si verifica una discrepanza tra gli orari dichiarati in cui si verificano le operazioni (ad esempio le istantanee) e gli orari effettivi in cui si verificano le operazioni.
Modifica della configurazione del server NTP	Specificare **2**. Ti viene richiesto di fornire una configurazione del server NTP.
Visualizzazione della configurazione del server NTP	Specificare **3**. Viene visualizzata la configurazione del server NTP.

Esecuzione di comandi relativi alla manutenzione per l'agente

Nella console locale dell' DataSync agente, è possibile eseguire alcune attività di manutenzione e diagnosticare problemi con l'agente.

Per eseguire un comando di configurazione o diagnostica nella console locale dell'agente

1. Accedi alla console locale del tuo agente.
2. Nel menu principale AWS DataSync Attivazione - Configurazione, immettete **5** (o **6** per una VMware macchina virtuale) il prompt dei comandi.
3. Usa i seguenti comandi per eseguire le seguenti attività con il tuo agente.

Comando	Descrizione
`dig`	Cerca informazioni DNS sull'host.

Comando	Descrizione
diskclean	Esegui la pulizia del disco.
exit	Torna al menu di configurazione della console.
h	Visualizza un elenco di comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete.
ip	Visualizza o configura routing, dispositivi e tunnel.
iptables	Configura e gestisci il filtraggio dei IPv4 pacchetti e il NAT.
ip6tables	Configura e gestisci il filtraggio dei IPv6 pacchetti e il NAT.
ncport	Verifica la connettività a una porta TCP di rete specifica.
nping	Ottieni informazioni per risolvere i problemi di rete.
passwd	Cambia la password dell'utente.
save-iptables	Salva le regole del firewall della IPv4 tabella in modo permanente.
save-ip6tables	Salva le regole del firewall della IPv6 tabella in modo permanente.
save-routing-table	Salva una voce della tabella di routing appena aggiunta.
sslcheck	Verifica se un certificato SSL è valido.
tcptraceroute	Raccogli `traceroute` l'output sul traffico TCP verso una destinazione.

4. Segui le istruzioni sullo schermo.

Sostituire il tuo AWS DataSync agente

Per sostituire un AWS DataSync agente, è necessario creare un nuovo agente e aggiornare tutte le sedi di trasferimento che utilizzano il vecchio agente.

Creazione di un nuovo agente

Per creare un nuovo DataSync agente, segui la stessa procedura utilizzata per creare il vecchio agente:

1. Implementa un agente nel tuo ambiente di storage.
2. Scegli un endpoint di servizio con cui l'agente comunica. AWS
3. Configura la rete in modo che l'agente possa comunicare con lo storage e AWS.
4. Attiva il tuo agente.
5. Una volta attivato, prendi nota dell'Amazon Resource Name (ARN) dell'agente.

   È necessario questo ARN quando si aggiorna la DataSync posizione per utilizzare il nuovo agente.

Aggiornamento della posizione con il nuovo agente

Dopo aver creato un nuovo agente, puoi aggiornare una DataSync sede esistente per utilizzare questo agente. Nella maggior parte dei casi, è inoltre necessario reinserire le credenziali di accesso per aggiornare la posizione. Questo perché DataSync archivia le credenziali di localizzazione in modo che solo l'agente possa utilizzarle.

Utilizzo della console DataSync

Le seguenti istruzioni descrivono come aggiornare le posizioni con un nuovo agente utilizzando la DataSync console.

NFS

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.

3. Scegli la posizione che desideri aggiornare, quindi scegli Modifica.
4. Per gli agenti, scegli il tuo nuovo agente.

   Puoi scegliere più di un agente se sostituisci più agenti per una sede.
5. Scegli Save changes (Salva modifiche).

SMB

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.
3. Scegli la posizione che desideri aggiornare, quindi scegli Modifica.
4. Per gli agenti, scegli il tuo nuovo agente.

   Puoi scegliere più di un agente se sostituisci più agenti per una sede.
5. Per Password, inserisci la password dell'utente che può installare il file server SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.
6. Scegli Save changes (Salva modifiche).

HDFS

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.
3. Scegli la posizione che desideri aggiornare, quindi scegli Modifica.
4. Per gli agenti, scegli il tuo nuovo agente.

   Puoi scegliere più di un agente se sostituisci più agenti per una sede.
5. Se utilizzi l'autenticazione Kerberos, carica il file Keytab e il file di configurazione Kerberos.
6. Scegli Save changes (Salva modifiche).

Object storage

1. Apri la console all'indirizzo. AWS DataSync https://console.aws.amazon.com/datasync/
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.
3. Scegli la posizione che desideri aggiornare, quindi scegli Modifica.

4. Per gli agenti, scegli il tuo nuovo agente.

   Puoi scegliere più di un agente se sostituisci più agenti per una sede.
5. Se la tua posizione richiede credenziali, inserisci la chiave segreta che consente di accedere DataSync al tuo bucket di archiviazione degli oggetti.
6. Scegli Save changes (Salva modifiche).

Azure Blob Storage

Effettua le seguenti operazioni per aggiornare il tuo Microsoft Azure Blob Storage ubicazione:

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.
3. Scegli la posizione che desideri aggiornare, quindi scegli Modifica.
4. Per gli agenti, scegli il tuo nuovo agente.

   Puoi scegliere più di un agente se sostituisci più agenti per una sede.
5. Per il token SAS, inserisci il token SAS (Shared Access Signature) che DataSync consente di accedere allo storage BLOB.
6. Scegli Save changes (Salva modifiche).

Utilizzando il AWS CLI

Le seguenti istruzioni descrivono come aggiornare le sedi con un nuovo agente utilizzando il AWS CLI. (Puoi farlo anche utilizzando l'DataSync API.)

NFS

1. Copia il seguente update-location-nfscomando:

   ```
   aws datasync update-location-nfs \
     --location-arn datasync-nfs-location-arn \
     --on-prem-config AgentArns=new-datasync-agent-arn
   ```
2. Per il `--location-arn` parametro, specifica l'ARN della posizione NFS che stai aggiornando.
3. Per l'`AgentArns`opzione del `--on-prem-config` parametro, specifica l'ARN del tuo nuovo agente.

Puoi specificare più di un ARN se stai sostituendo più agenti per una sede.

4. Esegui il `update-location-nfs` comando per aggiornare la posizione.

SMB

1. Copia il seguente update-location-smbcomando:

```
aws datasync update-location-smb \
  --location-arn datasync-smb-location-arn \
  --agent-arns new-datasync-agent-arn \
  --password smb-file-server-password
```

2. Per il `--location-arn` parametro, specifica l'ARN della posizione SMB che stai aggiornando.
3. Per il `--agent-arns` parametro, specifica l'ARN del tuo nuovo agente.

   Puoi specificare più di un ARN se stai sostituendo più agenti per una sede.
4. Per il `--password` parametro, specificate la password dell'utente che può montare il file server SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento.
5. Eseguite il `update-location-smb` comando per aggiornare la posizione.

HDFS

1. Copia il seguente update-location-hdfscomando:

```
aws datasync update-location-hdfs \
  --location-arn datasync-hdfs-location-arn \
  --agent-arns new-datasync-agent-arn \
  --kerberos-keytab keytab-file \
  --kerberos-krb5-conf krb5-conf-file
```

2. Per il `--location-arn` parametro, specifica l'ARN della posizione HDFS che stai aggiornando.
3. Per il `--agent-arns` parametro, specifica l'ARN del tuo nuovo agente.

   Puoi specificare più di un ARN se stai sostituendo più agenti per una sede.

4. Se utilizzi l'autenticazione Kerberos, includi i `--kerberos-keytab` parametri e: `--kerberos-krb5-conf`

   - Per il `--kerberos-keytab` parametro, specifica la tabella delle chiavi Kerberos (keytab) che contiene le mappature tra il principale Kerberos definito e le chiavi crittografate.

     È possibile specificare il file keytab fornendo l'indirizzo del file.

   - Per il `--kerberos-krb5-conf` parametro, specifica il file che contiene la configurazione per il tuo realm Kerberos.

     È possibile specificare il `krb5.conf` file fornendo l'indirizzo del file.

   Se utilizzi l'autenticazione semplice, non è necessario includere questi parametri relativi a Kerberos nel comando.

5. Esegui il `update-location-hdfs` comando per aggiornare la posizione.

Object storage

1. Copia il seguente update-location-object-storagecomando:

   ```
   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. Per il `--location-arn` parametro, specificate l'ARN della posizione di archiviazione degli oggetti che state aggiornando.

3. Per il `--agent-arns` parametro, specifica l'ARN del tuo nuovo agente.

   Puoi specificare più di un ARN se stai sostituendo più agenti per una sede.

4. Effettuate le seguenti operazioni a seconda che la posizione di archiviazione degli oggetti richieda credenziali di accesso:

   - Se la posizione richiede credenziali: per il `--secret-key` parametro, specifica la chiave segreta che consente di accedere DataSync al bucket di archiviazione degli oggetti.
   - Se la tua posizione richiede credenziali, specifica delle stringhe vuote per i parametri and. `--access-key` `--secret-key` Ecco un comando di esempio:

```
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. Esegui il `update-location-object-storage` comando per aggiornare la posizione.

Azure Blob Storage

1. Copia il seguente update-location-azure-blobcomando:

```
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. Per il `--location-arn` parametro, specificare l'ARN del Azure Blob Storage posizione che stai aggiornando.
3. Per il `--agent-arns` parametro, specifica l'ARN del tuo nuovo agente.

   Puoi specificare più di un ARN se stai sostituendo più agenti per una sede.
4. Per l'`Token`opzione del `--sas-configuration` parametro, specifica il token SAS che consente di accedere DataSync al tuo archivio BLOB.
5. Esegui il `update-location-azure-blob` comando per aggiornare la posizione.

Passaggi successivi

1. Elimina il tuo vecchio agente. Se hai delle DataSync attività in esecuzione che utilizzano questo agente, attendi il completamento di tali attività prima di eliminarle.
2. Se devi sostituire agenti per più sedi, ripeti i passaggi precedenti.
3. Quando hai finito, puoi riprendere a eseguire le tue attività.

> **Note**
>
> Sostituzione di agenti per attività pianificate: se sostituisci un agente per un'attività pianificata, devi avviare l'attività manualmente se il nuovo agente utilizza un tipo di endpoint di servizio diverso rispetto al vecchio agente. Se non si esegue l'operazione manualmente prima della successiva esecuzione pianificata, l'operazione ha esito negativo.
> Ad esempio, se il vecchio agente utilizzava un endpoint di servizio pubblico, ma il nuovo agente utilizza un endpoint VPC, avvia l'attività manualmente utilizzando la console o l'operazione. `StartTaskExecution` Dopodiché, l'attività riprenderà a funzionare secondo la pianificazione.

Filtraggio delle risorse AWS DataSync

Puoi filtrare le tue AWS DataSync sedi e le tue attività utilizzando le operazioni `ListLocations` e `ListTasks` API in AWS CLI. Ad esempio, recupera un elenco delle tue attività più recenti.

Parametri per il filtraggio

Puoi utilizzare i filtri API per restringere l'elenco delle risorse restituite da `ListTasks` and`ListLocations`. Ad esempio, per recuperare tutte le tue sedi Amazon S3, puoi `ListLocations` utilizzare il nome del filtro `LocationType` *`S3`*e. `Operator` *`Equals`*

Per filtrare i risultati dell'API, devi specificare un nome, un operatore e un valore del filtro.

- `Name`— Il nome del filtro che viene utilizzato. Ogni chiamata API supporta un elenco di filtri disponibili (ad esempio, `LocationType` per`ListLocations`).
- `Values`— I valori in base ai quali si desidera filtrare. Ad esempio, potresti voler visualizzare solo le sedi Amazon S3.
- `Operator`— L'operatore utilizzato per confrontare i valori dei filtri (ad esempio, `Equals` o`Contains`).

La tabella seguente elenca gli operatori disponibili.

Operatore	Tipi di chiave
`Equals`	Stringa, numero
`NotEquals`	Stringa, numero
`LessThan`	Numero
`LessThanOrEqual`	Numero
`GreaterThan`	Numero
`GreaterThanOrEqual`	Numero
`In`	Stringa
`Contains`	Stringa
`NotContains`	Stringa
`BeginsWith`	Stringa

Filtraggio per località

`ListLocations`supporta i seguenti nomi di filtro:

- `LocationType`— Filtri in base al tipo di posizione:
  - `SMB`
  - `NFS`
  - `HDFS`
  - `OBJECT_STORAGE`
  - `S3`
  - `OUTPOST_S3`
  - `FSX_WINDOWS`
  - `FSX_LUSTRE`
  - `FSX_OPENZFS_NFS`
  - `FSX_ONTAP_NFS`

  - `FSX_ONTAP_SMB`
- `LocationUri`— Filtri sull'URI (Uniform Resource Identifier) assegnato alla posizione, come restituito dalla chiamata `DescribeLocation*` API (ad esempio, `s3://bucket-name/your-prefix` per le sedi Amazon S3).
- `CreationTime`— Filtri in base all'ora in cui la posizione è stata creata. Il formato di input è `yyyy-MM-dd:mm:ss` in UTC (Coordinated Universal Time).

L' AWS CLI esempio seguente elenca tutte le posizioni di tipo Amazon S3 che hanno un URI di posizione che inizia con la stringa `"s3://amzn-s3-demo-bucket"` e che sono state create alle 17:15:20 UTC del 15/12/2019 o successivamente.

```
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=GreaterThanOrEqual}]
```

Questo comando restituisce un output simile al seguente.

```
{
    "Locations": [
        {
            "LocationArn": "arn:aws:datasync:us-east-1:111122223333:location/
loc-333333333abcdef0",
            "LocationUri": "s3://amzn-s3-demo-bucket1/"
        },
        {
            "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-987654321abcdef0",
            "LocationUri": "s3://amzn-s3-demo-bucket2/"
        }
    ]
}
```

Filtraggio per attività

`ListTasks`supporta i seguenti nomi di filtro.

- `LocationId`— Filtri sulle posizioni di origine e di destinazione sui valori di Amazon Resource Name (ARN).

- `CreationTime`— Filtri in base all'ora in cui l'attività è stata creata. Il formato di input è `yyyy-MM-dd:mm:ss` in UTC.

L' AWS CLI esempio seguente mostra la sintassi utilizzata per il filtraggio. `LocationId`

```
aws datasync list-tasks \
    --filters Name=LocationId,Values=arn:aws:datasync:us-east-1:your-account-id:location/your-location-id,Operator=Contains
```

L'output di questo comando è simile al seguente.

```
{
    "Tasks": [
        {
            "TaskArn": "arn:aws:datasync:us-east-1:your-account-id:task/your-task-id",
            "Status": "AVAILABLE",
            "Name": "amzn-s3-demo-bucket"
        }
    ]
}
```

Pulizia delle AWS DataSync risorse

Se le hai utilizzate AWS DataSync per un test o non hai bisogno delle AWS risorse che hai creato, eliminale in modo che non ti vengano addebitati costi per le risorse che non intendi utilizzare.

> **Note**
>
> Se disponi di DataSync risorse disattivate in un'area di attivazione, tali risorse non vengono eliminate automaticamente. Le risorse sono ancora disponibili se abiliti nuovamente quella regione.

Eliminazione di un agente DataSync

Quando elimini un agente da AWS DataSync, la risorsa agente non è più associata al tuo Account AWS e non può essere annullata.

Tieni presente che l'eliminazione di un agente da DataSync non rimuove la relativa macchina virtuale (VM) o l' EC2 istanza Amazon dal tuo ambiente di storage. Puoi eliminare la macchina virtuale o l'istanza o riutilizzarla per attivare un nuovo agente.

Prerequisiti

Non eliminare un agente finché non aggiorni o rimuovi le DataSync risorse che dipendono da esso. Se stai sostituendo un agente, aggiorna le sedi di trasferimento con il nuovo agente. Se non sostituisci un agente, elimina prima le attività e le sedi di trasferimento utilizzando quell'agente.

Eliminazione dell'agente

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, scegli Agenti.
3. Scegli l'agente che desideri eliminare.
4. Scegli Elimina, inserisci **`delete`** nella casella di testo che appare, quindi scegli Elimina.
5. Se non hai intenzione di riutilizzare l'infrastruttura dell'agente per altre DataSync attività, elimina la macchina virtuale o l' EC2 istanza Amazon dell'agente per rimuoverla dal tuo ambiente di storage.

Riutilizzo dell'infrastruttura di un agente DataSync

Puoi eliminare una risorsa agente DataSync e continuare a utilizzare la macchina virtuale o l' EC2 istanza Amazon sottostante dell'agente per attivare un nuovo agente.

Per riutilizzare l'infrastruttura di un agente

1. Verifica la connessione dell'agente a. AWS Se i test di rete hanno esito positivo, vai al passaggio successivo.

   I test di rete devono essere superati prima di poter passare alla fase successiva.
2. Elimina la risorsa agente da DataSync ma non elimina la macchina virtuale o l' EC2 istanza Amazon dell'agente.
3. Ripeti il passaggio 1 per testare AWS nuovamente la connessione dell'agente. Se i test di rete hanno esito positivo, vai al passaggio successivo.

4. Circa tre minuti dopo aver eliminato la risorsa agente da DataSync, controlla se la porta 80 è aperta sulla macchina virtuale dell'agente o sull'istanza Amazon EC2 . Se lo è, vai al passaggio successivo.
5. Attiva un nuovo agente con la macchina virtuale o l' EC2 istanza Amazon esistente.

   Puoi attivare il nuovo agente in un altro Regione AWS tipo di endpoint di servizio e con un altro tipo di endpoint. Account AWS Se si utilizza un tipo diverso di endpoint di servizio, è necessario modificare la configurazione di rete.

Eliminazione di una posizione DataSync

Come procedura consigliata, rimuovi le AWS DataSync sedi che non ti servono più.

Per rimuovere una posizione utilizzando la DataSync console

1. Aprire la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.
3. Scegli la posizione che desideri rimuovere.
4. Scegli Elimina. Conferma l'eliminazione inserendo**`delete`**, quindi scegli Elimina.

Eliminazione di un'attività DataSync

Se non hai più bisogno di un' AWS DataSync attività, puoi eliminarla e AWS le relative risorse.

Prerequisiti

Quando si esegue un'attività, crea e gestisce DataSync automaticamente le interfacce di rete per il traffico di trasferimento dati. Quando si elimina un'attività, si eliminano anche le relative interfacce di rete, purché si disponga delle seguenti autorizzazioni:

- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`

Queste autorizzazioni sono disponibili nella politica gestita AWS . `AWSDataSyncFullAccess` Per ulteriori informazioni, consulta AWS politiche gestite per AWS DataSync.

Eliminazione dell'attività

Una volta eliminata un'attività, non è possibile ripristinarla.

Utilizzo della DataSync console

1. Apri la AWS DataSync console all'indirizzo https://console.aws.amazon.com/datasync/.
2. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Attività.
3. Seleziona l'attività che desideri eliminare.
4. Selezionare Actions (Operazioni), quindi selezionare Delete (Elimina).
5. Nella finestra di dialogo, scegli Delete (Elimina).

Usando il AWS CLI

1. Copia il seguente `delete-task` comando:

```
aws datasync delete-task \
      --task-arn "task-to-delete"
```

2. Per il `--task-arn` parametro, specifica l'Amazon Resource Name (ARN) dell'attività che stai eliminando (ad esempio,). `arn:aws:datasync:us-east-2:123456789012:task/task-012345678abcd0123`
3. Esegui il comando `delete-task`.

Sicurezza in AWS DataSync

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano a AWS DataSync, consulta Servizi AWS coperti dal programma di compliance.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo DataSync. I seguenti argomenti mostrano come eseguire la configurazione DataSync per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere DataSync le tue risorse.

Argomenti

- Protezione dei dati in AWS DataSync
- Gestione delle identità e degli accessi in AWS DataSync
- Convalida della conformità per AWS DataSync
- Resilienza in AWS DataSync
- Sicurezza dell'infrastruttura in AWS DataSync
- Protezione delle credenziali della posizione di archiviazione

Protezione dei dati in AWS DataSync

AWS DataSync trasferisce in modo sicuro i dati tra sistemi di storage autogestiti e servizi AWS di storage e anche tra servizi AWS di storage. Il modo in cui i dati di archiviazione vengono crittografati durante il trasferimento dipende in parte dalle località coinvolte nel trasferimento.

Una volta completato il trasferimento, i dati inattivi vengono crittografati dal sistema o dal servizio che li archivia (non DataSync).

Argomenti

- AWS DataSync crittografia in transito
- AWS DataSync crittografia a riposo
- Riservatezza del traffico Internet

AWS DataSync crittografia in transito

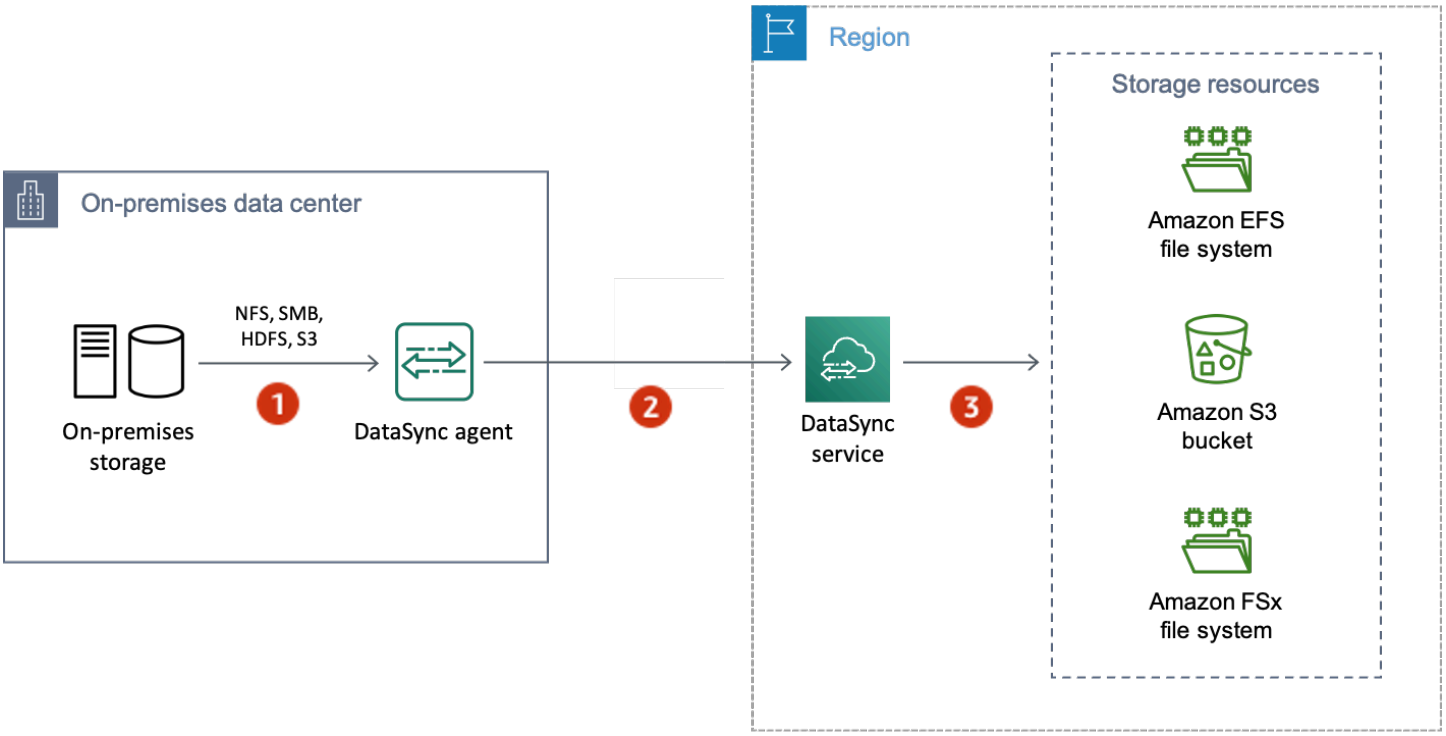
I dati di archiviazione (inclusi i metadati) vengono crittografati in transito, ma il modo in cui vengono crittografati durante il trasferimento dipende dalle posizioni di origine e destinazione.

Quando si connette a una località, DataSync utilizza le opzioni più sicure fornite dal protocollo di accesso ai dati di quella località. Ad esempio, quando ci si connette a un file system utilizzando Server Message Block (SMB), DataSync utilizza le funzionalità di sicurezza fornite da SMB.

Connessioni di rete in un trasferimento

DataSync richiede tre connessioni di rete per copiare i dati: una per leggere i dati da una posizione di origine, un'altra per trasferire dati tra posizioni e un'altra per scrivere dati in una posizione di destinazione.

Il diagramma seguente è un esempio delle connessioni di rete DataSync utilizzate per trasferire dati da un sistema di storage locale a un servizio di AWS storage. Per capire dove avvengono le connessioni e come vengono protetti i dati durante il trasferimento tramite ciascuna connessione, utilizza la tabella allegata.



Documentazione di riferimento	Connessione di rete	Descrizione
1	Lettura dei dati dalla posizione di origine	DataSync si connette utilizzando il protocollo del sistema di storage per l'accesso ai dati (ad esempio, SMB o l'API Amazon S3). Per questa connessione, i dati vengono protetti utilizzando le funzionalità di sicurezza del sistema di storage, a meno che DataSync non supporti tali funzional ità. Ad esempio, DataSync attualmen te non supporta l'autenticazione Kerberos con file server NFS o quando utilizza la crittografia TDE con HDFS.
2	Trasferimento di dati tra sedi	Per questa connessione, DataSync crittografa tutto il traffico di rete con

Documentazione di riferimento	Connessione di rete	Descrizione
		Mutual Transport Layer Security (mTLS) 1.3.
3	Scrittura dei dati nella posizione di destinazione	Analogamente alla posizione di origine, DataSync si connette utilizzando il protocollo del sistema di storage per l'accesso ai dati. I dati vengono nuovamente protetti utilizzando le funzionalità di sicurezza del sistema di storage, a meno che DataSync non supporti tali funzional ità.

Scopri come i tuoi dati vengono crittografati in transito quando ti DataSync connetti ai seguenti servizi AWS di archiviazione:

- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP
- Amazon S3

Crittografie TLS

Durante il trasferimento di dati tra sedi, DataSync utilizza diversi cifrari TLS. La crittografia TLS dipende dal tipo di endpoint di servizio con cui l'agente comunica. DataSync Per ulteriori informazioni, consulta Scelta di un endpoint di servizio per il tuo agente AWS DataSync.

Indice

- Endpoint pubblici o VPC
- Endpoint FIPS

Endpoint pubblici o VPC

Per gli endpoint del servizio cloud privato pubblico e virtuale (VPC), DataSync utilizza uno dei seguenti cifrari TLS:

- SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_ (ecdh_x25519)
- TLS_ECDHE_RSA_CON_ 0_ 05_ (ecdh_x25519CHACHA2) POLY13 SHA256
- TLS_ECDHE_RSA_CON_AES_128_GCM_ (ECDH_x25519SHA256)

Endpoint FIPS

Per gli endpoint del servizio Federal Information Processing Standard (FIPS), utilizza il seguente codice TLS: DataSync

- SHA256 TLS_AES_128_GCM_ (secp256r1)

AWS DataSync crittografia a riposo

AWS DataSync Trattandosi di un servizio di trasferimento, in genere non gestisce i dati di archiviazione inattivi. I servizi e i sistemi di archiviazione che lo DataSync supportano sono responsabili della protezione dei dati in tale stato. Tuttavia, alcuni dati relativi ai servizi vengono DataSync gestiti a riposo.

Cosa è crittografato?

Gli unici dati DataSync archiviati riguardano i dettagli necessari per completare il trasferimento. DataSync archivia i seguenti dati con crittografia completa a riposo in Amazon DynamoDB:

- configurazioni delle attività (ad esempio, dettagli sulle ubicazioni del trasferimento).
- Credenziali utente che consentono all' DataSync agente di autenticarsi presso una sede. Queste credenziali vengono crittografate utilizzando le chiavi pubbliche dell'agente. L'agente può decrittografare queste chiavi secondo necessità con le sue chiavi private.

Per ulteriori informazioni, consulta DynamoDB encryption at rest nella Amazon DynamoDB Developer Guide.

Gestione delle chiavi

Non è possibile gestire le chiavi di crittografia DataSync utilizzate per archiviare le informazioni in DynamoDB relative all'esecuzione dell'attività. Queste informazioni includono le configurazioni delle attività e le credenziali utilizzate dagli agenti per l'autenticazione con una posizione di archiviazione.

Cosa non è crittografato?

Sebbene DataSync non controlli il modo in cui i dati di archiviazione vengono crittografati quando sono archiviati, consigliamo comunque di configurare le sedi con il massimo livello di sicurezza da esse supportato. Ad esempio, puoi crittografare oggetti con chiavi di crittografia gestite Amazon S3 (SSE-S3) AWS Key Management Service o chiavi (KMS) (AWS SSE-KMS).

Scopri di più su come i servizi di storage crittografano i dati inattivi: AWS

- Amazon S3
- Amazon EFS
- File server Amazon FSx per Windows
- Amazon FSx per Lustre
- Amazon FSx per OpenZFS
- Amazon FSx per NetApp ONTAP

Riservatezza del traffico Internet

Ti consigliamo di configurare le posizioni di origine e di destinazione con il massimo livello di sicurezza supportato da ciascuna di esse. Quando ci si connette a una posizione, AWS DataSync funziona con la versione più sicura del protocollo di accesso ai dati utilizzata dal sistema di storage. Inoltre, è consigliabile limitare il traffico di sottorete a protocolli e servizi noti.

DataSync protegge la connessione tra le posizioni, incluse quelle tra e le zone di disponibilità Account AWS Regioni AWS, utilizzando Transport Layer Security (TLS) 1.3.

Gestione delle identità e degli accessi in AWS DataSync

AWS utilizza credenziali di sicurezza per identificarti e concederti l'accesso alle tue risorse. AWS Puoi utilizzare le funzionalità di AWS Identity and Access Management (IAM) per consentire ad altri

utenti, servizi e applicazioni di utilizzare le tue AWS risorse completamente o in modo limitato, senza condividere le tue credenziali di sicurezza.

Per impostazione predefinita, le identità IAM (utenti, gruppi e ruoli) non dispongono dell'autorizzazione per creare, visualizzare o modificare le AWS risorse. Per consentire a utenti, gruppi e ruoli di accedere alle AWS DataSync risorse e interagire con la DataSync console e l'API, ti consigliamo di utilizzare una policy IAM che conceda loro l'autorizzazione a utilizzare le risorse e le azioni API specifiche di cui avranno bisogno. Quindi devi collegare la policy all'identità IAM che richiede l'accesso. Per una panoramica degli elementi di base di una policy, consulta Gestione degli accessi per AWS DataSync.

Argomenti

- Gestione degli accessi per AWS DataSync
- AWS politiche gestite per AWS DataSync
- Politiche gestite dai clienti IAM per AWS DataSync
- Utilizzo di ruoli collegati ai servizi per DataSync
- Autorizzazioni per l' DataSync etichettatura delle risorse durante la creazione
- Prevenzione del problema "confused deputy" tra servizi

Gestione degli accessi per AWS DataSync

Ogni AWS risorsa è di proprietà di un. Account AWS Le autorizzazioni per creare o accedere a una risorsa sono regolate dalle policy di autorizzazione. Un amministratore di account può allegare politiche di autorizzazione alle identità AWS Identity and Access Management (IAM). Alcuni servizi (ad esempio AWS Lambda) supportano anche l'associazione di politiche di autorizzazione alle risorse.

> **Note**
>
> Un amministratore di account è un utente con privilegi di amministratore in un. Account AWS Per ulteriori informazioni, consultare la sezione best practice IAM nella Guida per l'utente IAM.

Argomenti

- DataSync risorse e operazioni

- Informazioni sulla proprietà delle risorse
- Gestione dell'accesso alle risorse
- Specifica degli elementi delle policy: operazioni, effetti, risorse ed entità
- Specifica delle condizioni in una policy

DataSync risorse e operazioni

In DataSync, le risorse principali sono agente, ubicazione, attività ed esecuzione dell'attività.

A queste risorse sono associati Amazon Resource Names (ARNs) univoci, come illustrato nella tabella seguente.

Tipo di risorsa	Formato ARN
ARN agente	`arn:aws:datasync:` *`region`*`:`*`account-id`* `:agent/`*`agent-id`*
ARN posizione	`arn:aws:datasync:` *`region`*`:`*`account-id`* `:location/` *`location-id`*
ARN attività	`arn:aws:datasync:` *`region`*`:`*`account-id`* `:task/`*`task-id`*
ARN di esecuzione delle attività	`arn:aws:datasync:` *`region`*`:`*`account-id`* `:task/`*`task-id`*`/execution/` *`exec-id`*

Per concedere le autorizzazioni per operazioni API specifiche, come la creazione di un'attività, DataSync definisce una serie di azioni che è possibile specificare in una politica di autorizzazioni. Un'operazione API può richiedere le autorizzazioni per più di un'operazione.

Informazioni sulla proprietà delle risorse

Il proprietario della risorsa è colui Account AWS che ha creato la risorsa. Cioè, il proprietario Account AWS della risorsa è l'entità principale (ad esempio, un ruolo IAM) che autentica la richiesta che crea la risorsa. Gli esempi seguenti illustrano come funziona questo comportamento:

- Se usi le credenziali dell'account root del tuo account Account AWS per creare un'attività, sei il proprietario della risorsa (in DataSync, la risorsa è l'attività). Account AWS

- Se crei un ruolo IAM nel tuo Account AWS e concedi le autorizzazioni per l'`CreateTask`azione a quell'utente, l'utente può creare un'attività. Tuttavia Account AWS, la risorsa dell'attività è di proprietà dell'utente a cui appartiene.
- Se crei un ruolo IAM Account AWS con le autorizzazioni necessarie per creare un'attività, chiunque possa assumere il ruolo può creare un'attività. Il tuo Account AWS, a cui appartiene il ruolo, possiede la risorsa dell'attività.

Gestione dell'accesso alle risorse

La policy delle autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

> **Note**
>
> Questa sezione illustra l'utilizzo di IAM nel contesto di DataSync. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione di IAM completa, consulta la pagina Che cos'è IAM? nella Guida per l'utente di IAM. Per informazioni sulla sintassi e le descrizioni delle policy IAM, consulta il riferimento alle AWS Identity and Access Management policy nella IAM User Guide.

Le politiche associate a un'identità IAM sono denominate politiche basate sull'identità (politiche IAM) e le politiche allegate a una risorsa sono denominate politiche basate sulle risorse. DataSync supporta solo politiche basate sull'identità (politiche IAM).

Argomenti

- Policy basate sull'identità
- Policy basate sulle risorse

Policy basate sull'identità

Puoi gestire l'accesso alle DataSync risorse con le policy IAM. Queste policy possono aiutare un Account AWS amministratore a fare quanto segue con DataSync:

- Concedi le autorizzazioni per creare e gestire DataSync risorse: crea una policy IAM che consenta a un ruolo IAM Account AWS all'interno dell'azienda di creare e gestire DataSync risorse, come agenti, sedi e attività.

- Concedi le autorizzazioni a un ruolo in un altro Account AWS o in un altro Servizio AWS: crea una policy IAM che conceda le autorizzazioni a un ruolo IAM in un altro o in un altro. Account AWS Servizio AWS Per esempio:

  1. L'amministratore dell'Account A crea un ruolo IAM e attribuisce una politica di autorizzazioni al ruolo che concede le autorizzazioni sulle risorse nell'Account A.
  2. L'amministratore dell'Account A attribuisce una politica di fiducia al ruolo che identifica l'Account B come principale che può assumere il ruolo.

     Per concedere l' Servizio AWS autorizzazione ad assumere il ruolo, l'amministratore dell'Account A può specificare un Servizio AWS come principale nella politica di fiducia.
  3. L'amministratore dell'Account B può quindi delegare le autorizzazioni per assumere il ruolo a qualsiasi utente dell'Account B. Ciò consente a chiunque utilizzi il ruolo nell'Account B di creare o accedere alle risorse nell'Account A.

  Per ulteriori informazioni sull'uso di IAM per delegare le autorizzazioni, consultare Gestione degli accessi nella Guida per l'utente di IAM.

La politica di esempio seguente concede le autorizzazioni a tutte le azioni su tutte le risorse`List*`. Questa azione è di sola lettura e non consente la modifica delle risorse.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllListActionsOnAllResources",
            "Effect": "Allow",
            "Action": [
                "datasync:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni sull'utilizzo delle politiche basate sull'identità con DataSync, consulta le politiche gestite e le politiche AWS gestite dai clienti. Per ulteriori informazioni sulle identità IAM, consulta la IAM User Guide.

Policy basate sulle risorse

Altri servizi, come Amazon S3, supportano politiche di autorizzazione basate sulle risorse. Ad esempio, è possibile associare una policy a un bucket Amazon S3 per gestire le autorizzazioni di accesso a quel bucket. Tuttavia, DataSync non supporta politiche basate sulle risorse.

Specifica degli elementi delle policy: operazioni, effetti, risorse ed entità

Per ogni DataSync risorsa, il servizio definisce una serie di operazioni API (vedi Azioni). Per concedere le autorizzazioni per queste operazioni API, DataSync definisce una serie di azioni che è possibile specificare in una politica. Ad esempio, per la DataSync risorsa, vengono definite le seguenti azioni:`CreateTask`,`DeleteTask`, e`DescribeTask`. L'esecuzione di un'operazione API può richiedere le autorizzazioni per più di un'operazione.

Di seguito sono elencati gli elementi di base di una policy:

- Risorsa: in una policy si utilizza il nome della risorsa Amazon (ARN) per identificare la risorsa a cui si applica la policy stessa. Per le risorse DataSync, puoi utilizzare il carattere jolly (*) nelle policy IAM. Per ulteriori informazioni, consulta DataSync risorse e operazioni.
- Operazione: utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, a seconda dell'`Effect`elemento specificato, l'`datasync:CreateTask`autorizzazione consente o nega all'utente le autorizzazioni per eseguire l' DataSync `CreateTask`operazione.
- Effetto: si specifica l'effetto quando l'utente richiede l'azione specifica. Questo effetto può essere o. `Allow` `Deny` Se non concedi esplicitamente l'accesso a (`Allow`) una risorsa, l'accesso viene negato implicitamente. Puoi anche negare esplicitamente l'accesso a una risorsa, cosa che potresti fare per assicurarti che un utente non possa accedervi, anche se una politica diversa concede a quell'utente l'accesso. Per ulteriori informazioni, consulta Authorization nella IAM User Guide.
- Principale: nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per le politiche basate sulle risorse, specifica l'utente, l'account, il servizio o l'altra entità a cui desideri ricevere le autorizzazioni (si applica solo alle politiche basate sulle risorse). DataSync non supporta politiche basate sulle risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta il riferimento alle AWS Identity and Access Management policy nella IAM User Guide.

Specifica delle condizioni in una policy

Quando concedi le autorizzazioni, puoi usare il linguaggio delle policy IAM per specificare le condizioni in base alle quali applicare una policy. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni sulla specificazione delle condizioni nel linguaggio delle policy, consulta Condition nella IAM User Guide.

Per esprimere le condizioni è necessario utilizzare chiavi di condizione predefinite. Non esistono chiavi di condizione specifiche per DataSync. Tuttavia, ci sono AWS ampi tasti di condizione che puoi usare a seconda delle esigenze. Per un elenco completo delle chiavi AWS ampie, consulta Available keys in the IAM User Guide.

AWS politiche gestite per AWS DataSync

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scriverle autonomamente. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

Servizi AWS mantenere e aggiornare le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy `ReadOnlyAccess` AWS gestita fornisce l'accesso in sola lettura a tutte le Servizi AWS risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AWSDataSyncReadOnlyAccess

È possibile allegare la policy `AWSDataSyncReadOnlyAccess` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura per. DataSync

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DataSyncReadOnlyAccessPermissions",
        "Effect": "Allow",
        "Action": [
            "datasync:Describe*",
            "datasync:List*",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "elasticfilesystem:DescribeFileSystems",
            "elasticfilesystem:DescribeMountTargets",
            "fsx:DescribeFileSystems",
            "iam:GetRole",
            "iam:ListRoles",
            "logs:DescribeLogGroups",
            "logs:DescribeResourcePolicies",
            "s3:ListAllMyBuckets",
            "s3:ListBucket"
        ],
        "Resource": "*"
    }]
}
```

AWS politica gestita: AWSDataSyncFullAccess

È possibile allegare la policy `AWSDataSyncFullAccess` alle identità IAM.

Questa politica concede le autorizzazioni amministrative DataSync ed è necessaria per AWS Management Console l'accesso al servizio. `AWSDataSyncFullAccess`fornisce l'accesso completo alle operazioni DataSync API e alle operazioni che interagiscono con le risorse correlate (come bucket Amazon S3, file system Amazon EFS, AWS KMS chiavi e segreti di Secrets Manager). La policy concede anche autorizzazioni per Amazon CloudWatch, tra cui la creazione di gruppi di log e la creazione o l'aggiornamento di una politica sulle risorse.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DataSyncFullAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "datasync:*",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcEndpoints",
                "ec2:ModifyNetworkInterfaceAttribute",
                "fsx:DescribeFileSystems",
                "fsx:DescribeStorageVirtualMachines",
                "elasticfilesystem:DescribeAccessPoints",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeMountTargets",
                "iam:GetRole",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "logs:DescribeResourcePolicies",
                "outposts:ListOutposts",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3-outposts:ListAccessPoints",
                "s3-outposts:ListRegionalBuckets",
```

```
                "secretsmanager:ListSecrets",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DataSyncPassRolePermissions",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "DataSyncCreateSLRPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "datasync.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DataSyncSecretsManagerCreateAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
            ],
            "Resource": [
                "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "DataSyncSecretsManagerAccess",
            "Effect": "Allow",
            "Action": [

                "secretsmanager:DeleteSecret",
                "secretsmanager:UpdateSecret",
                "secretsmanager:PutSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:aws-datasync!*"
            ],
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/
aws:secretsmanager:owningService": "aws-datasync",
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
         }
    ]
}
```

AWS politica gestita: AWSDataSyncServiceRolePolicy

Non puoi collegare la `AWSDataSyncServiceRolePolicy` policy alle tue identità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di eseguire azioni DataSync per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per DataSync.

Questa politica concede autorizzazioni amministrative che consentono al ruolo collegato al servizio di creare CloudWatch log Amazon per le attività che utilizzano la modalità Enhanced. DataSync

Aggiornamenti alle policy

Modifica	Descrizione	Data
AWSDataSyncFullAccess— Modifica	DataSync dichiarazioni di autorizzazione modificate per`AWSDataSyncFullAccess` : Le istruzioni aggiornate rimuovono le condizioni di etichettatura dai permessi DataSync utilizzati per creare segreti di Secrets Manager.	13 maggio 2025
AWSDataSyncFullAccess— Cambia	DataSync ha aggiunto nuove autorizzazioni a`AWSDataSyncFullAccess` : • `secretsmanager:CreateSecret` • `secretsmanager:PutSecretValue` • `secretsmanager:DeleteSecret` • `secretsmanager:UpdateSecret` Queste autorizzazioni consentono di DataSync creare, modificare ed eliminare AWS Secrets Manager segreti.	7 maggio 2025
AWSDataSyncFullAccess— Cambia	DataSync ha aggiunto nuove autorizzazioni a`AWSDataSyncFullAccess` :	23 aprile 2025

Modifica	Descrizione	Data
	• `secretsmanager:ListSecrets` • `kms:ListAliases` • `kms:DescribeKey` Queste autorizzazioni consentono di DataSync recuperare i metadati relativi ai AWS Secrets Manager segreti e alle AWS KMS chiavi, inclusi eventuali alias associati alle chiavi.	
AWSDataSyncServiceRolePolicy— Cambia	DataSync ha aggiunto nuove autorizzazioni alla `AWSDataSyncServiceRolePolicy` politica utilizzata dal ruolo collegato al DataSync servizio: `AWSServiceRoleForDataSync` • `secretsmanager:DescribeSecret` • `secretsmanager:GetSecretValue` Queste autorizzazioni consentono di DataSync leggere i metadati e i valori dei segreti gestiti da. AWS Secrets Manager	15 aprile 2025

Modifica	Descrizione	Data
AWSDataSyncService RolePolicy: nuova policy	DataSync ha aggiunto una politica utilizzata dal ruolo collegato al DataSync servizio. `AWSServiceRoleForDataSync` Questa nuova policy gestita crea automaticamente CloudWatch i log Amazon per le tue DataSync attività che utilizzano la modalità Enhanced.	30 ottobre 2024
AWSDataSyncFullAccess— Modifica	DataSync ha aggiunto una nuova autorizzazione a `AWSDataSyncFullAccess` : • `iam:CreateServiceLinkedRole` Questa autorizzazione consente di DataSync creare per te ruoli collegati ai servizi.	30 ottobre 2024
AWSDataSyncFullAccess— Modifica	DataSync ha aggiunto una nuova autorizzazione a `AWSDataSyncFullAccess` : • `ec2:DescribeRegions` Questa autorizzazione consente di scegliere regioni opzionali quando si crea un' DataSync attività per i trasferimenti tra Regioni AWS.	22 luglio 2024

Modifica	Descrizione	Data
AWSDataSyncFullAccess— Modifica	DataSync ha aggiunto una nuova autorizzazione a`AWSDataSyncFullAccess` : • `s3:ListBucketVersions` Questa autorizzazione ti consente di scegliere una versione specifica del tuo DataSync manifesto.	16 febbraio 2024

Modifica	Descrizione	Data
AWSDataSyncFullAccess— Modifica	DataSync ha aggiunto nuove autorizzazioni a`AWSDataSyncFullAccess` : • `ec2:DescribeVpcEndpoints` • `elasticfilesystem:DescribeAccessPoints` • `fsx:DescribeStorageVirtualMachines` • `outposts:ListOutposts` • `s3:GetBucketLocation` • `s3-outposts:ListAccessPoints` • `s3-outposts:ListRegionalBuckets` Queste autorizzazioni ti aiutano a creare DataSync agenti e sedi per Amazon EFS, Amazon FSx for NetApp ONTAP, Amazon S3 e S3 on Outposts.	2 maggio 2023
DataSync ha iniziato a tenere traccia delle modifiche	DataSync ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	1 marzo 2021

Politiche gestite dai clienti IAM per AWS DataSync

Oltre alle policy AWS gestite, puoi anche creare policy personalizzate basate sull'identità AWS DataSync e collegarle alle identità AWS Identity and Access Management (IAM) che richiedono tali autorizzazioni. Queste sono note come politiche gestite dai clienti, che sono politiche autonome che puoi amministrare autonomamente. Account AWS

> **Important**
>
> Prima di iniziare, ti consigliamo di conoscere i concetti e le opzioni di base per la gestione dell'accesso alle tue DataSync risorse. Per ulteriori informazioni, consulta Gestione degli accessi per AWS DataSync.

Quando si crea una politica gestita dai clienti, si includono dichiarazioni sulle DataSync operazioni che possono essere utilizzate su determinate AWS risorse. La politica di esempio seguente contiene due istruzioni (notate gli `Resource` elementi `Action` e in ogni istruzione):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllTasks",
            "Effect": "Allow",
            "Action": [
                "datasync:DescribeTask",
            ],
            "Resource": "arn:aws:datasync:us-east-2:111222333444:task/*"
        },
        {
            "Sid": "ListAllTasks",
            "Effect": "Allow",
            "Action": [
                "datasync:ListTasks"
            ],
            "Resource": "*"
        },
}
```

Le dichiarazioni della politica fanno quanto segue:

- La prima istruzione concede le autorizzazioni per eseguire l'`datasync:DescribeTask`azione su determinate risorse dell'attività di trasferimento specificando un Amazon Resource Name (ARN) con un carattere jolly (). *
- La seconda istruzione concede le autorizzazioni per eseguire l'`datasync:ListTasks`azione su tutte le attività specificando solo un carattere jolly (). *

Esempi di politiche gestite dai clienti

L'esempio seguente di politiche gestite dai clienti concedono autorizzazioni per varie DataSync operazioni. Le politiche funzionano se utilizzi AWS Command Line Interface (AWS CLI) o un AWS SDK. Per utilizzare queste politiche nella console, devi utilizzare anche la policy `AWSDataSyncFullAccess` gestita.

Argomenti

- Esempio 1: crea una relazione di fiducia che DataSync consenta di accedere al tuo bucket Amazon S3
- Esempio 2: consenti DataSync di leggere e scrivere nel tuo bucket Amazon S3
- Esempio 3: consenti di DataSync caricare i log in gruppi di log CloudWatch

Esempio 1: crea una relazione di fiducia che DataSync consenta di accedere al tuo bucket Amazon S3

Di seguito è riportato un esempio di policy di fiducia che consente di DataSync assumere un ruolo IAM. Questo ruolo consente di accedere DataSync a un bucket Amazon S3. Per evitare il problema della confusione tra diversi servizi, consigliamo di utilizzare le chiavi di contesto `aws:SourceArn`e di contesto della condizione `aws:SourceAccount`globale contenute nella policy.

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:*"
                }
            }
        }
    ]
}
```

Esempio 2: consenti DataSync di leggere e scrivere nel tuo bucket Amazon S3

La seguente politica di esempio concede DataSync le autorizzazioni minime per leggere e scrivere dati su un bucket S3 utilizzato come posizione di destinazione.

> **Note**
>
> Il valore per `aws:ResourceAccount` deve essere l'ID dell'account proprietario del bucket Amazon S3 specificato nella policy.

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

Esempio 3: consenti di DataSync caricare i log in gruppi di log CloudWatch

DataSync richiede le autorizzazioni per poter caricare i log nei tuoi gruppi di CloudWatch log Amazon. Puoi utilizzare i gruppi di CloudWatch log per monitorare ed eseguire il debug delle tue attività.

Per un esempio di policy IAM che concede tali autorizzazioni, vedi. Consentire DataSync il caricamento dei log in un gruppo di CloudWatch log

Utilizzo di ruoli collegati ai servizi per DataSync

AWS DataSync utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. DataSync I ruoli collegati ai servizi sono predefiniti DataSync e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Argomenti

- Utilizzo dei ruoli per DataSync

Utilizzo dei ruoli per DataSync

AWS DataSync utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. DataSync I ruoli collegati ai servizi sono predefiniti DataSync e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione DataSync perché non è necessario aggiungere manualmente le autorizzazioni necessarie. DataSync definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. DataSync Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi DataSync le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

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

Autorizzazioni di ruolo collegate ai servizi per DataSync

DataSync utilizza il ruolo collegato al servizio denominato AWSServiceRoleForDataSync: consente DataSync di eseguire operazioni essenziali per l'esecuzione delle attività di trasferimento, tra cui la lettura di informazioni segrete e la creazione CloudWatch di gruppi di AWS Secrets Manager log ed eventi.

Il ruolo AWSService RoleForDataSync collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `datasync.amazonaws.com`

Il ruolo collegato al servizio utilizza la policy AWS gestita denominata AWSDataSyncServiceRolePolicy, che consente di DataSync completare le seguenti azioni sulle risorse specificate:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DataSyncCloudWatchLogCreateAccess",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:*:logs:*:*:log-group:/aws/datasync*"
            ]
        },
        {
            "Sid": "DataSyncCloudWatchLogStreamUpdateAccess",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
            ]
        },
        {
            "Sid": "DataSyncSecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DescribeSecret",
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
            ],
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/
aws:secretsmanager:owningService": "aws-datasync",
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
```

```
    ]
}
```

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per DataSync

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un' DataSync attività in AWS Management Console, the o nell' AWS API AWS CLI, DataSync crea automaticamente il ruolo collegato al servizio.

Nell'API AWS CLI o nell' AWS API, puoi creare un ruolo collegato al servizio con il nome del servizio. `datasync.amazonaws.com` Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente di IAM. Se elimini il ruolo collegato ai servizi, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un' DataSync attività, DataSync crea nuovamente il ruolo collegato al servizio per te.

Se elimini questo ruolo collegato al servizio, puoi utilizzare lo stesso processo IAM per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per DataSync

DataSync non consente di modificare il ruolo collegato al AWSService RoleForDataSync servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per DataSync

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

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo.

> **Note**
>
> Se il DataSync servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare DataSync le risorse utilizzate da AWSService RoleForDataSync

1. Eliminare gli DataSync agenti utilizzati dall'attività (se presenti).
2. Eliminare le posizioni dell'attività.
3. Eliminare l'attività.

Eliminazione manuale del ruolo collegato ai servizi

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSService RoleForDataSync collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi DataSync

DataSync supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta AWS Regioni ed endpoint.

Autorizzazioni per l' DataSync etichettatura delle risorse durante la creazione

Alcune azioni AWS DataSync API per la creazione di risorse consentono di specificare i tag quando si crea la risorsa. È possibile utilizzare i tag delle risorse per implementare il controllo degli accessi basato sugli attributi (ABAC). Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

Per consentire agli utenti di etichettare le risorse al momento della creazione, devono disporre delle autorizzazioni per utilizzare l'azione che crea la risorsa (ad esempio `datasync:CreateAgent`

o`datasync:CreateTask`). Se i tag sono specificati nell'azione di creazione della risorsa, gli utenti devono inoltre disporre di autorizzazioni esplicite per utilizzare l'azione. `datasync:TagResource`

L'operazione `datasync:TagResource` viene valutata solo se i tag vengono applicati durante l'operazione di creazione di risorse. Pertanto, un utente che dispone delle autorizzazioni per creare una risorsa (presupponendo che non vi siano condizioni di etichettatura) non richiede le autorizzazioni per utilizzare l'`datasync:TagResource`eazione se nella richiesta non sono specificati tag.

Tuttavia, se l'utente tenta di creare una risorsa con tag, la richiesta fallisce se l'utente non dispone delle autorizzazioni per utilizzare l'azione. `datasync:TagResource`

Esempi di dichiarazioni politiche IAM

Utilizza il seguente esempio di istruzioni politiche IAM per concedere `TagResource` autorizzazioni agli utenti che creano DataSync risorse.

La seguente istruzione consente agli utenti di taggare un DataSync agente quando lo creano.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:444455556666:agent/*"
        }
    ]
}
```

L'istruzione seguente consente agli utenti di taggare una DataSync posizione quando la creano.

JSON

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

```
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:111122223333:location/*"
        }
    ]
}
```

L'istruzione seguente consente agli utenti di etichettare un' DataSync attività quando la creano.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:444455556666:task/*"
        }
    ]
}
```

Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione intersettoriale può portare al confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Si consiglia di utilizzare `aws:SourceArn` le chiavi di contesto della condizione `aws:SourceAccount` globale nelle politiche delle risorse per limitare le autorizzazioni che AWS DataSync forniscono un altro servizio alla risorsa. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore

`aws:SourceAccount` e l'account nel valore `aws:SourceArn` deve utilizzare lo stesso ID account nella stessa dichiarazione di policy. Utilizzare `aws:SourceArn` se si desidera consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri che qualsiasi risorsa in quell'account sia associata all'uso tra servizi.

Il valore di `aws:SourceArn` deve includere l'ARN della DataSync posizione con cui DataSync è consentito assumere il ruolo IAM.

Il modo più efficace per proteggersi dal confuso problema del vice è utilizzare la `aws:SourceArn` chiave con l'ARN completo della risorsa. Se non conosci l'ARN completo o se stai specificando più risorse, usa i caratteri jolly (*) per le parti sconosciute. Ecco alcuni esempi di come eseguire questa operazione per: DataSync

- Per limitare la politica di attendibilità a una DataSync posizione esistente, includi l'ARN completo della posizione nella policy. DataSync assumerà il ruolo IAM solo quando avrà a che fare con quella particolare posizione.
- Quando crei una sede Amazon S3 per DataSync, non conosci l'ARN della posizione. In questi scenari, usa il seguente formato per la `aws:SourceArn` chiave:. `arn:aws:datasync:`*`us-east-2`*`:`*`123456789012`*`:*` Questo formato convalida la partizione (`aws`), l'ID account e la regione.

L'esempio completo seguente mostra come è possibile utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition in una politica di fiducia per evitare il confuso problema del vice. DataSync

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:*"
                }
            }
        }
    ]
}
```

Per ulteriori esempi di policy che mostrano come utilizzare `aws:SourceArn` le chiavi di contesto della condizione `aws:SourceAccount` globale con DataSync, consultate i seguenti argomenti:

- Crea una relazione di fiducia che DataSync consenta di accedere al tuo bucket Amazon S3
- Configura un ruolo IAM per accedere al tuo bucket Amazon S3

Convalida della conformità per AWS DataSync

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.

- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS DataSync

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

> **Note**
>
> Se una zona di disponibilità verso o da cui state migrando i dati fallisce durante l'esecuzione di un' DataSync attività, anche l'operazione fallirà.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta infrastruttura AWS globale.

Sicurezza dell'infrastruttura in AWS DataSync

In quanto servizio gestito, AWS DataSync è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere DataSync attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Protezione delle credenziali della posizione di archiviazione

DataSync utilizza le posizioni per accedere alle risorse di archiviazione situate in sede, in altri cloud o in. AWS Alcuni tipi di ubicazione richiedono l'immissione di credenziali, come una chiave di accesso e una chiave segreta o un nome utente e una password, per l'autenticazione con il sistema di storage. Quando si crea una DataSync posizione che richiede credenziali per l'autenticazione, è possibile scegliere una delle seguenti opzioni per controllare la modalità di archiviazione del segreto delle credenziali:

- Memorizza il segreto AWS Secrets Manager utilizzando un segreto gestito dal servizio crittografato con una chiave predefinita.
- Memorizza il segreto AWS Secrets Manager utilizzando un segreto gestito dal servizio crittografato con una AWS KMS chiave gestita da te.
- Memorizza il segreto AWS Secrets Manager utilizzando un segreto e una chiave creati e gestiti da te. DataSync accede a questo segreto utilizzando un ruolo IAM fornito da te.

In tutti i casi, il segreto di Secrets Manager viene memorizzato nel tuo account, consentendoti di aggiornarlo secondo necessità, indipendentemente dal DataSync servizio. Ti viene addebitato solo l'uso di segreti che crei al di fuori di DataSync. I segreti creati e gestiti da DataSync hanno il prefissoaws-datasync.

Utilizzo di un segreto gestito dal servizio crittografato con una chiave predefinita

Quando crei la tua DataSync posizione, devi semplicemente fornire la stringa segreta. DataSynccrea una risorsa segreta AWS Secrets Manager per archiviare il segreto fornito e lo crittografa con la chiave KMS Secrets Manager predefinita per il tuo account. Puoi modificare il valore segreto direttamente in Secrets Manager o aggiornando la posizione utilizzando la DataSync console o AWS CLI l'SDK. Quando elimini la risorsa di localizzazione o la aggiorni per utilizzare un segreto personalizzato, DataSync elimina automaticamente la risorsa segreta.

> **Note**
>
> Per creare, modificare ed eliminare risorse segrete in Secrets Manager, è DataSync necessario disporre delle autorizzazioni appropriate. Per ulteriori informazioni, consulta Policy gestite da AWS per DataSync.

Utilizzo di un segreto gestito dal servizio crittografato con una chiave personalizzata AWS KMS

Quando crei la tua DataSync posizione, fornisci il segreto e l'ARN della tua AWS KMS chiave. DataSync crea automaticamente una risorsa segreta in AWS Secrets Manager cui archiviare il segreto fornito e lo cripta utilizzando la tua AWS KMS chiave. Puoi modificare il valore segreto direttamente in Secrets Manager o aggiornando la posizione utilizzando la DataSync console o AWS CLI l'SDK. Quando elimini la risorsa di localizzazione o la aggiorni per utilizzare un segreto personalizzato, DataSync elimina automaticamente la risorsa segreta.

> **Note**
>
> La AWS KMS chiave deve utilizzare la crittografia simmetrica con il ENCRYPT_DECRYPT tipo di chiave. Per ulteriori informazioni, consulta Scelta di una AWS Key Management Service chiave nella Guida per l'AWS Secrets Manager utente.

Per creare, modificare ed eliminare risorse segrete in Secrets Manager, è DataSync necessario disporre delle autorizzazioni appropriate. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSDataSyncFullAccess.

Oltre a utilizzare la politica DataSync gestita corretta, sono necessarie anche le seguenti autorizzazioni:

```
{
    "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*Sostituiscilo con la tua chiave KMS ARN.

Per recuperare e decrittografare il valore segreto, DataSync utilizza un Service Linked Role (SLR) per accedere alla chiave. AWS KMS Per assicurarti di DataSync poter utilizzare la tua chiave KMS, aggiungi quanto segue alla dichiarazione sulla politica della chiave:

```
{
    "Sid": "Allow DataSync to use the key for decryption",
    "Effect": "Allow",
    "Principal": {
            "AWS": "arn:aws:iam::accountid:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

*accountid*Sostituiscila con il tuo Account AWS ID.

Usando un segreto che gestisci

Prima di creare la tua DataSync posizione, crea un indirizzo segreto. AWS Secrets Manager Il valore del segreto deve contenere solo la stringa segreta stessa in testo semplice. Quando crei la tua DataSync posizione, fornisci l'ARN del tuo segreto e un ruolo IAM che DataSync utilizza per accedere sia al tuo segreto che alla AWS KMS chiave utilizzata per crittografare il tuo segreto. Per creare un ruolo IAM con le autorizzazioni appropriate, procedi come segue:

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli, quindi scegli Crea ruolo.
3. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli AWS servizio.
4. Per Caso d'uso, scegli DataSyncdall'elenco a discesa. Scegli Next (Successivo).
5. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo). Inserisci un nome per il tuo ruolo, quindi scegli Crea ruolo.
6. Nella pagina Ruoli, cerca il ruolo che hai appena creato e scegline il nome.
7. Nella pagina Dettagli del ruolo, scegli la scheda Autorizzazioni. Scegli Aggiungi autorizzazioni, quindi Crea politica in linea.
8. Scegli la scheda JSON e aggiungi le seguenti autorizzazioni nell'editor delle politiche:

   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"
        }
    ]
}
```

Sostituisci *your-secret-arn* con l'ARN del tuo segreto di Secrets Manager.

9. Scegli Next (Successivo). Inserisci un nome per la tua politica, quindi scegli Crea politica.
10. (Consigliato) Per evitare il problema del sostituto confuso tra diversi servizi, procedi come segue:

    a. Nella pagina Dettagli del ruolo, scegli la scheda Relazioni fiduciarie. Seleziona Modifica policy di attendibilità.

    b. Aggiorna la politica di fiducia utilizzando l'esempio seguente, che include le chiavi del contesto `aws:SourceArn` e della condizione `aws:SourceAccount` globale:

    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. Scegli Aggiorna policy.

Puoi specificare questo ruolo durante la creazione della tua sede. Se il tuo segreto utilizza una AWS KMS chiave gestita dal cliente per la crittografia, dovrai anche aggiornare la politica della chiave per

consentire l'accesso dal ruolo creato nella procedura precedente. Per aggiornare la politica, aggiungi quanto segue alla dichiarazione sulla politica della tua AWS KMS chiave:

```
{
    "Sid": "Allow DataSync use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam accountid:role/your-role-name”
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

Sostituiscila *accountid* con il tuo Account AWS ID e *your-role-name* con il nome del ruolo IAM che hai creato nella procedura precedente.

> **Note**
>
> Quando memorizzi segreti in Secrets Manager, ti vengono Account AWS addebitati dei costi. Per informazioni sui prezzi, consulta Prezzi di AWS Secrets Manager.

AWS DataSync quote

Scopri le quote e i limiti delle risorse quando lavori con AWS DataSync.

Limiti del sistema di storage, dei file e degli oggetti

La tabella seguente descrive i limiti che si DataSync hanno quando si lavora con sistemi di storage, file e oggetti.

Descrizione	Limite
Lunghezza massima totale del percorso del file	4,096 byte
Lunghezza massima del componente del percorso del file (nome del file, directory o sottodirectory)	255 byte
Lunghezza massima del dominio Windows	253 caratteri
Lunghezza massima del nome host del server	255 caratteri
Lunghezza massima del nome dell'oggetto Amazon S3	1.024 caratteri UTF-8

DataSync quote

La tabella seguente descrive le quote di DataSync risorse in una regione Account AWS e in una regione specifica.

Risorsa	Quota	Regolabile
Numero massimo di attività che è possibile creare	100	Sì
(Attività in modalità avanzata) Numero massimo di oggetti di origine e destinazione	Praticamente illimitato	N/D

Risorsa	Quota	Regolabile
con cui DataSync è possibile lavorare per esecuzione di attività Per ulteriori informazioni, consulta Come DataSync trasferisce file, oggetti e directory		

Risorsa	Quota	Regolabile
(Attività in modalità base) Numero massimo di file, oggetti e directory di origine e destinazione DataSync utilizzabili per ogni operazione tra servizi di archiviazione e archiviazione locali, autogestiti o di altro tipo AWS Per ulteriori informazioni, consulta Come DataSync trasferisce file, oggetti e directory	50 milioni **Important** Ricorda quanto segue su questa quota: • Se trasferisci oggetti Amazon S3 con prefissi, i prefissi vengono trattati come directory e conteggiati ai fini della quota. Ad esempio, DataSync `s3://bucket/foo/bar.txt` consideriamo due directory (`./`and) e `./foo/` un oggetto (). `bar.txt` • Se la tua attività prevede l'utilizzo di più di 20 milioni di file, oggetti o directory, assicurati di allocare almeno 64 GB di RAM al tuo agente. DataSync Per ulteriori informazioni, consulta i requisiti degli agenti	Sì **Tip** Invece di richiedere un aumento, puoi creare attività incentrate su directory specifiche utilizzando i filtri di inclusione ed esclusione. Per ulteriori informazioni, consulta Filtraggio dei dati trasferiti da. DataSync

Risorsa	Quota	Regolabile
	per DataSync i trasferimenti.	

Risorsa	Quota	Regolabile
(Attività in modalità base) Numero massimo di file, oggetti e directory di origine e destinazione utilizzabili DataSync per ogni operazione eseguita tra i AWS servizi di storage Per ulteriori informazioni, consulta Come DataSync trasferisce file, oggetti e directory	25 milioni **Important** Se trasferisci oggetti Amazon S3 con prefissi, i prefissi vengono trattati come directory e conteggiati ai fini della quota. Ad esempio, DataSync `s3://bucket/foo/bar.txt` considera due directory (`./` and) e `./foo/` un oggetto (). `bar.txt`	Sì **Tip** Invece di richiedere un aumento, è possibile creare attività incentrate su directory specifiche utilizzando i filtri di inclusione ed esclusione. Per ulteriori informazioni, consulta Filtraggio dei dati trasferit

Risorsa	Quota	Regolabile
		i da. DataSync
Velocità effettiva massima per attività (per i trasferimenti che utilizzano un DataSync agente)	10 Gb/s	No
Velocità effettiva massima per attività (per i trasferimenti che non utilizzano un DataSync agente)	5 Gb/s	No
Numero massimo di caratteri che è possibile includere in un filtro delle attività	102.400 caratteri **Note** Se utilizzi la DataSync console, questo limite include tutti i caratteri combinati nei modelli di inclusione ed esclusione.	No
Numero massimo di esecuzioni in coda per una singola attività	50	No
Numero massimo di esecuzioni simultanee di attività in modalità avanzata	120	No
Numero massimo di giorni in cui viene conservata la cronologia dell'esecuzione di un'attività	30	No

Richiesta di un aumento della quota

È possibile richiedere un aumento per alcune DataSync quote. Gli aumenti non vengono concessi immediatamente e potrebbero essere necessari un paio di giorni prima che abbiano effetto.

Richiesta di un aumento delle quote

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.
2. Nel riquadro di navigazione, scegli AWS servizi, quindi scegli AWS DataSync.
3. Scegli la quota che desideri aumentare, quindi scegli Richiedi aumento a livello di account.
4. Inserisci l'importo totale che desideri sia la quota, quindi scegli Richiedi.

   Se devi aumentare una quota diversa, compila una richiesta separata.

Risoluzione dei AWS DataSync problemi

Utilizza le seguenti informazioni per risolvere problemi ed errori AWS DataSync .

Argomenti

- Risoluzione dei problemi con gli agenti DataSync
- Risoluzione dei problemi relativi alle DataSync sedi
- Risoluzione dei problemi relativi alle DataSync attività
- Risoluzione dei problemi di verifica dei dati
- Risoluzione dei problemi relativi ai costi di storage S3 superiori al previsto con DataSync

Risoluzione dei problemi con gli agenti DataSync

Utilizza le seguenti informazioni per aiutarti a risolvere i problemi relativi agli AWS DataSync agenti. Alcuni di questi problemi possono includere:

- Problemi di connessione alla console locale di un EC2 agente Amazon
- Impossibile recuperare la chiave di attivazione di un agente
- Problemi di attivazione di un agente con un endpoint di servizio VPC
- La scoperta di un agente è offline

Come posso connettermi alla console locale di un EC2 agente Amazon?

Per connetterti alla console locale di un EC2 agente Amazon, devi usare SSH. Assicurati che il gruppo di sicurezza dell' EC2 istanza consenta l'accesso con SSH (porta TCP 22).

In un terminale, esegui il seguente `ssh` comando per connetterti all'istanza:

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

- Per*`/path/key-pair-name`*, specifica il percorso e il nome del file (`.pem`) della chiave privata richiesta per connetterti all'istanza.
- Per *`instance-user-name`*, specificare `admin`.
- Per*`instance-public-ip-address`*, specifica l'indirizzo IP pubblico dell'istanza.

Cosa significa l'errore Failed to retrieve activation key dell'agente?

Quando si attiva l' DataSync agente, l'agente si connette all'endpoint del servizio specificato per richiedere una chiave di attivazione. Questo errore indica probabilmente che le impostazioni di sicurezza della rete stanno bloccando la connessione.

Operazione da eseguire

Se utilizzi un endpoint del servizio Virtual Private Cloud (VPC), verifica che le impostazioni del gruppo di sicurezza consentano all'agente di connettersi all'endpoint VPC. Per informazioni sulle porte richieste, consulta Requisiti di rete per gli endpoint del servizio VPC.

Se utilizzi un endpoint pubblico o FIPS (Federal Information Processing Standard), verifica che le impostazioni del firewall e del router consentano all'agente di connettersi all'endpoint. Per informazioni, consultare Requisiti di rete per gli endpoint di servizio pubblici o FIPS.

Non riesco ancora ad attivare un agente utilizzando un endpoint del servizio VPC

Se continui a riscontrare problemi nell'attivazione di un DataSync agente con un endpoint di servizio VPC, consulta Non so cosa stia succedendo con il mio agente. Qualcuno può aiutarmi?

Cosa devo fare se il mio agente è offline?

Il tuo DataSync agente può essere offline per alcuni motivi, ma potresti riuscire a ripristinarlo. Prima di eliminare l'agente e crearne uno nuovo, consulta la seguente lista di controllo per aiutarti a capire cosa potrebbe essere successo.

- Contatta il tuo team di backup: se l'agente è offline perché la sua macchina virtuale (VM) è stata ripristinata da un'istantanea o da un backup, potrebbe essere necessario sostituire l'agente.
- Verifica se la macchina virtuale o l' EC2 istanza Amazon dell'agente è disattivata: a seconda del tipo di agente che stai utilizzando, prova a riaccendere la macchina virtuale o l' EC2 istanza se è disattivata. Una volta riacceso, verifica la connettività di rete del tuo agente a. AWS
- Verifica che l'agente soddisfi i requisiti hardware minimi: l'agente potrebbe essere offline perché la configurazione della macchina virtuale o dell' EC2 istanza è stata modificata accidentalmente dopo l'attivazione dell'agente. Ad esempio, se la macchina virtuale non dispone più della memoria o dello spazio minimi richiesti, l'agente potrebbe apparire offline. Per ulteriori informazioni, consulta Requisiti per gli agenti AWS DataSync.

- Attendi il completamento degli aggiornamenti software relativi all'agente: l'agente potrebbe andare offline per un breve periodo dopo gli aggiornamenti software forniti da. AWS Se ritieni che questo sia il motivo per cui l'agente è offline, attendi un breve periodo, quindi controlla se l'agente è tornato online.
- Controlla le impostazioni dell'endpoint del servizio VPC: se il tuo agente offline utilizza un endpoint di servizio pubblico e si trova anche nello stesso VPC per cui hai creato un endpoint del servizio VPC DataSync, potresti dover disabilitare il supporto DNS privato per quell'endpoint VPC.

Se nessuna di queste sembra essere la ragione per cui l'agente è offline, probabilmente dovrai sostituirlo.

Non so cosa stia succedendo con il mio agente. Qualcuno può aiutarmi?

Puoi consentire l'accesso Supporto AWS al tuo DataSync agente e contribuire alla risoluzione dei problemi relativi all'agente. È necessario abilitare questo accesso tramite la console locale dell'agente.

Per fornire Supporto l'accesso al tuo agente

1. Accedi alla console locale del tuo agente.
2. Al prompt, inserisci **5** per aprire il prompt dei comandi (for VMware VMs, use**6**).
3. Immettere **h** per aprire la finestra AVAILABLE COMMANDS (COMANDI DISPONIBILI).
4. Nella finestra COMANDI DISPONIBILI, inserisci quanto segue per connetterti a: Supporto

   ```
   open-support-channel
   ```

   Se utilizzi l'agente con endpoint VPC, devi fornire un indirizzo IP dell'endpoint VPC per il tuo canale di supporto, come segue:

   ```
   open-support-channel vpc-ip-address
   ```

   Il firewall deve consentire alla porta TCP 22 in entrata di avviare un canale di supporto. AWS Quando ti connetti a Supporto, ti DataSync assegna un numero di supporto. che è bene annotare.

> **Note**
>
> Il numero del canale non è un numero di porta TCP/UDP. Al contrario, stabilisce una connessione SSH (TCP 22) ai server e fornisce il canale di supporto per la connessione.

5. Una volta stabilito il canale di supporto, fornisci il numero del servizio di supporto a Supporto in modo che possano fornire assistenza per la risoluzione dei problemi.
6. Quando la sessione di supporto è terminata, premi **`Enter`** per terminarla.
7. Entra **`exit`** per disconnetterti dalla console DataSync locale.
8. Seguire le istruzioni per uscire dalla console locale.

Risoluzione dei problemi relativi alle DataSync sedi

Utilizza le seguenti informazioni per aiutarti a risolvere i problemi relativi alle posizioni. AWS DataSync Alcuni di questi problemi possono includere:

- Autorizzazioni ed errori di montaggio con posizioni NFS
- Problemi di proprietà dei file
- Problemi di accesso alle sedi SMB che utilizzano l'autenticazione Kerberos
- Problemi di autorizzazione e accesso con lo storage di oggetti, come le ubicazioni Amazon S3 e Microsoft Azure Blob

La mia attività non è riuscita a causa di un errore NFS con autorizzazioni negate

Puoi ricevere il messaggio di errore «autorizzazioni negate» se configuri il tuo file server NFS con `root_squash` o `all_squash` e non tutti i tuoi file hanno accesso in lettura.

Operazione da eseguire

Per risolvere questo problema, configura l'esportazione NFS con `no_root_squash` o assicurati che le autorizzazioni per tutti i file che desideri trasferire consentano l'accesso in lettura a tutti gli utenti.

Per accedere DataSync alle directory, devi anche abilitare l'accesso a tutte le esecuzioni. Per assicurarsi che la directory possa essere montata, collegarsi innanzitutto a qualsiasi computer che dispone della stessa configurazione di rete dell'agente. Quindi esegui il seguente comando CLI:

```
mount -t nfs -o nfsvers=<your-nfs-server-version> <your-nfs-server-
name>:<nfs-export-path-you-specified> <new-test-folder-on-your-computer>
```

Se il problema persiste, contatta il Supporto AWS Centro.

La mia operazione non è riuscita a causa di un errore di montaggio NFS

È possibile che venga visualizzato il seguente errore durante l'esecuzione di un' DataSync attività che coinvolge una posizione del file server NFS:

Attività non riuscita ad accedere alla posizione loc-1111222233334444a: x40016: mount.nfs: Connessione scaduta

Operazioni da eseguire

Procedi come segue fino alla risoluzione dell'errore.

1. Assicuratevi che il file server NFS e l'esportazione specificati nella vostra DataSync posizione siano validi. In caso contrario, elimina la posizione e l'attività, quindi crea una nuova posizione e un'attività che utilizzino un file server NFS valido ed esportale. Per ulteriori informazioni, consulta Utilizzo della console di DataSync.
2. Controlla la configurazione del firewall tra l'agente e il file server NFS. Per ulteriori informazioni, consulta Requisiti di rete per lo storage locale, autogestito, su altri cloud ed edge.
3. Assicurati che il tuo agente possa accedere al file server NFS e montare l'esportazione. Per ulteriori informazioni, consulta Fornire DataSync l'accesso ai file server NFS.
4. Se l'errore persiste, apri un canale di supporto con Supporto. Per ulteriori informazioni, consulta Non so cosa stia succedendo con il mio agente. Qualcuno può aiutarmi?.

La mia attività non è riuscita a causa di un errore di montaggio di Amazon EFS

Potresti visualizzare il seguente errore durante l'esecuzione di un' DataSync attività che coinvolge una posizione Amazon EFS:

Attività non riuscita ad accedere alla posizione loc-1111222233334444a: x40016: connessione alla destinazione di montaggio EFS non riuscita con IP: 10.10.1.0.

Ciò può accadere se il percorso di montaggio del file system Amazon EFS che configuri con la tua posizione viene aggiornato o eliminato. DataSync non è a conoscenza di queste modifiche nel file system.

Operazione da eseguire

Elimina la posizione e l'attività e crea una nuova posizione Amazon EFS con il nuovo percorso di montaggio.

La proprietà dei file non viene mantenuta con NFS Transfer

Dopo il trasferimento, potreste notare che i file nella posizione di DataSync destinazione hanno utenti IDs (UIDs) o gruppi IDs (GIDs) diversi rispetto agli stessi file nella posizione di origine. Ad esempio, i file nella destinazione potrebbero avere un UID di `6553499`, `onobody`.

Ciò può accadere se un file system coinvolto nel trasferimento utilizza la mappatura ID NFS versione 4, una funzionalità che DataSync non supporta.

Operazione da eseguire

Hai un paio di opzioni per risolvere questo problema:

- Create una nuova posizione per il file system che utilizza la versione 3 di NFS anziché la versione 4.
- Disabilita la mappatura degli ID di NFS versione 4 sul file system.

Riprova il trasferimento. Entrambe le opzioni dovrebbero risolvere il problema.

La mia attività non può accedere a una sede SMB che utilizza Kerberos

DataSync gli errori nelle sedi SMB che utilizzano l'autenticazione Kerberos sono in genere correlati a mancate corrispondenze tra la posizione dell'utente e le configurazioni Kerberos. Potrebbe esserci anche un problema di rete.

Impossibile accedere alla posizione

L'errore seguente indica che potrebbero esserci problemi di configurazione con la sede SMB o la configurazione di Kerberos:

```
Task failed to access location
```

Verifica quanto segue:

- Il file server SMB specificato per la posizione è un nome di dominio. Per Kerberos, non è possibile specificare l'indirizzo IP del file server.
- Il principale Kerberos specificato per la propria posizione corrisponde al principale utilizzato per creare il file della tabella delle chiavi Kerberos (keytab). I nomi principali distinguono tra maiuscole e minuscole.
- La password utente mappata del preside Kerberos non è cambiata da quando è stato creato il file keytab. Se la password cambia (a causa della rotazione della password o per qualche altro motivo), l'esecuzione dell'operazione potrebbe non riuscire con il seguente errore:

  L'operazione non è riuscita ad accedere alla posizione loc-1111222233334444a: x40015: kinit: preautenticazione non riuscita durante l'acquisizione delle credenziali iniziali

Impossibile contattare KDC realm

Il seguente errore indica un problema di rete:

```
kinit: Cannot contact any KDC for realm 'MYDOMAIN.ORG' while getting initial
 credentials"
```

Verifica quanto segue:

- Il file di configurazione Kerberos (`krb5.conf`) che hai fornito DataSync contiene le informazioni corrette sul tuo realm Kerberos. Per un `krb5.conf` file di esempio, consulta Prerequisiti di autenticazione Kerberos.
- La porta del server Kerberos Key Distribution Center (KDC) è aperta. La porta KDC è in genere la porta TCP 88.
- La configurazione DNS sulla tua rete.

La mia operazione non è riuscita a causa di un input/output errore

È possibile che venga visualizzato un messaggio di input/output errore se il sistema di storage non soddisfa I/O le richieste dell' DataSync agente. I motivi più comuni includono un errore del disco del server, modifiche alla configurazione del firewall o un errore del router di rete.

Se l'errore riguarda un file server NFS o un cluster Hadoop Distributed File System (HDFS), utilizzate i seguenti passaggi per risolvere l'errore.

Azioni da intraprendere (NFS)

Innanzitutto, controllate i log e le metriche del vostro file server NFS per determinare se il problema è iniziato sul server NFS. In caso affermativo, risolvete il problema.

Quindi, verificare che la configurazione di rete non sia cambiata. Per verificare se il file server NFS è configurato correttamente e se è DataSync possibile accedervi, effettuate le seguenti operazioni:

1. Configurare un altro client NFS sulla stessa sottorete della rete dell'agente .
2. Montare la condivisione su tale client.
3. Convalidare che il client è in grado di leggere e scrivere correttamente nella condivisione.

Azioni da intraprendere (HDFS)

Effettua le seguenti operazioni fino a risolvere l'errore:

1. Assicurati che il cluster HDFS consenta all' DataSync agente di comunicare con il cluster NameNode e le DataNode porte.

   Nella maggior parte dei cluster, puoi trovare i numeri di porta utilizzati dal cluster nei seguenti file di configurazione:

   - Per trovare la NameNode porta, cercate nel `core-site.xml` file sotto la `fs.default.name` proprietà `fs.default` o (a seconda della distribuzione Hadoop).
   - Per trovare la DataNode porta, cerca nel `hdfs-site.xml` file sotto la `dfs.datanode.address` proprietà.
2. Nel `hdfs-site.xml` file, verifica che la `dfs.data.transfer.protection` proprietà abbia un solo valore. Per esempio:

   ```
   <property>
      <name>dfs.data.transfer.protection</name>
      <value>privacy</value>
   </property>
   ```

Errore: **`FsS3UnableToConnectToEndpoint`**

DataSync non riesci a connetterti alla tua posizione Amazon S3. Ciò potrebbe significare che il bucket S3 della sede non è raggiungibile o che la posizione non è configurata correttamente.

Effettua le seguenti operazioni fino a risolvere il problema:

- Verifica se DataSync riesci ad accedere al tuo bucket S3.
- Assicurati che la posizione sia configurata correttamente utilizzando la DataSync console o il funzionamento di DescribeLocationS3.

Errore: `FsS3HeadBucketFailed`

DataSync non riesci ad accedere al bucket S3 verso o da cui stai trasferendo. Verifica se DataSync dispone dell'autorizzazione per accedere al bucket utilizzando l'operazione Amazon HeadBucketS3. Se devi modificare le tue autorizzazioni, consulta. Fornire DataSync l'accesso ai bucket S3

L'operazione ha esito negativo con un `Unable to list Azure Blobs on the volume root` errore

Se l'operazione di DataSync trasferimento non riesce a causa di un `Unable to list Azure Blobs on the volume root` errore, potrebbe esserci un problema con il token SAS (Shared Access Signature) o con la rete dell'account di Azure archiviazione.

Operazioni da eseguire

Prova quanto segue ed esegui nuovamente l'operazione finché non risolvi il problema:

- Assicurati che il tuo token SAS disponga delle autorizzazioni giuste per accedere al tuoMicrosoft Azure Blob Storage.
- Se utilizzi il tuo DataSync agenteAzure, configura il tuo account di archiviazione per consentire l'accesso dalla rete virtuale in cui risiede l'agente.
- Se utilizzi il tuo agente su Amazon EC2, configura il firewall Azure di storage per consentire l'accesso dall'indirizzo IP pubblico dell'agente.

Per informazioni su come configurare la rete del tuo account di Azure archiviazione, consulta la Azure Blob Storagedocumentazione.

Errore: `FsAzureBlobVolRootListBlobsFailed`

Il token SAS (Shared Access Signature) DataSync utilizzato per accedere al tuo Microsoft Azure Blob Storage non dispone dell'autorizzazione List.

Per risolvere il problema, aggiorna la tua posizione con un token con l'autorizzazione List e prova a eseguire nuovamente l'attività.

Errore: **SrcLocHitAccess**

DataSync non riesco ad accedere alla tua posizione di origine. Verifica di DataSync avere il permesso di accedere alla posizione e prova a eseguire nuovamente l'operazione.

Errore: **SyncTaskErrorLocationNotAdded**

DataSync non riesco ad accedere alla tua posizione. Verifica di DataSync avere il permesso di accedere alla posizione e prova a eseguire nuovamente l'operazione.

Errore: **S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation**

Questo errore potrebbe essere correlato alle autorizzazioni IAM, alle policy dei bucket di Amazon S3, alle autorizzazioni o ad altri AWS KMS problemi di autorizzazione. Se ricevi questo errore, utilizza le seguenti informazioni per risolvere il problema:

- Risolvi gli errori di accesso negato (403 proibito) in Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service
- In che modo è possibile risolvere gli errori 403 Access Denied di Amazon S3? su AWS re:Post

L'operazione con posizione di origine S3 ha esito negativo con **HeadObject** o **GetObjectTagging** errore

Se stai trasferendo oggetti con una versione specifica IDs da un bucket S3, potresti visualizzare un errore relativo a o. `HeadObject` `GetObjectTagging` Ad esempio, ecco un errore relativo a: `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
```

Se riscontri uno di questi errori, verifica che il ruolo IAM DataSync utilizzato per accedere alla posizione di origine di S3 disponga delle seguenti autorizzazioni:

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

Se devi aggiornare il tuo ruolo con queste autorizzazioni, consulta. Creazione di un ruolo IAM DataSync per accedere alla tua posizione Amazon S3

Risoluzione dei problemi relativi alle DataSync attività

Utilizza le seguenti informazioni per aiutarti a risolvere i problemi relativi alle attività e all' AWS DataSync esecuzione delle attività. Questi problemi possono includere problemi di configurazione delle attività, esecuzioni di attività bloccate e il mancato trasferimento dei dati come previsto.

Errore: valore non valido SyncOption . Opzione: TransferMode,PreserveDeletedFiles, Valore: ALL, REMOVE.

Questo errore si verifica quando crei o modifichi DataSync un'attività e selezioni l'opzione Trasferisci tutti i dati e deselezioni l'opzione Conserva file eliminati.

Quando trasferisci tutti i dati, DataSync non scansiona la posizione di destinazione e non sa cosa eliminare.

L'esecuzione dell'operazione non riesce con un EniNotFounderrore

Questo errore si verifica se elimini una delle interfacce di rete dell'attività nel tuo cloud privato virtuale (VPC). Se l'operazione è pianificata o in coda, l'operazione avrà esito negativo se manca un'interfaccia di rete necessaria per il trasferimento dei dati.

Operazioni da eseguire

Sono disponibili le seguenti opzioni per risolvere questo problema:

- Riavviare manualmente l'operazione. Quando si esegue questa operazione, DataSync verranno create tutte le interfacce di rete mancanti necessarie per eseguire l'operazione.
- Se devi ripulire le risorse nel tuo VPC, assicurati di non eliminare le interfacce di rete relative a un' DataSync attività che stai ancora utilizzando.

Per visualizzare le interfacce di rete assegnate alla tua attività, esegui una delle seguenti operazioni:

- Usa l'operazione. DescribeTask È possibile visualizzare le interfacce di rete negli elementi `SourceNetworkInterfaceArns` e di `DestinationNetworkInterfaceArns` risposta.
- Nella EC2 console Amazon, cerca l'ID dell'attività (ad esempio`task-f012345678abcdef0`) per trovare le relative interfacce di rete.

- Valuta la possibilità di non eseguire le attività automaticamente. Ciò potrebbe includere la disabilitazione dell'accodamento o della pianificazione delle attività (tramite l'automazione DataSync o personalizzata).

L'esecuzione dell'operazione non riesce con l'errore «Impossibile allocare la memoria»

Quando l' DataSync operazione fallisce a causa dell'errore Cannot allocate memory, ciò può significare diverse cose.

Operazione da eseguire

Prova quanto segue finché non vedi più il problema:

- Se il trasferimento coinvolge un agente, assicurati che l'agente soddisfi i requisiti della macchina virtuale (VM) o dell' EC2 istanza Amazon.
- Suddividi il trasferimento in più attività utilizzando i filtri. È possibile che tu stia cercando di trasferire più file o oggetti di quelli che un'unica DataSync attività può gestire.
- Se il problema persiste, contatta Supporto.

L'operazione ha esito negativo **`Input/Output error`** per il file system Amazon FSx for NetApp ONTAP

Se l' DataSync operazione non riesce `Input/Output error` durante il trasferimento di dati con un file system Amazon FSx for NetApp ONTAP, può essere dovuto a uno o più dei seguenti problemi.

- Il volume FSx for ONTAP ha raggiunto la capacità massima di file. Ciò accade quando il numero di inode, o puntatori di file, disponibili su un volume è esaurito.
- Il volume FSx for ONTAP ha esaurito la capacità di archiviazione disponibile.

- L'esecuzione dell' DataSync operazione determinava un'eccessiva concomitanza di lettura/scrittura e consumava una percentuale molto elevata della capacità di throughput del file system.

Operazioni da eseguire

È possibile risolvere questo problema esaminando lo stato del volume FSx for ONTAP per determinare la causa sottostante.

Per determinare se il volume ha raggiunto la capacità massima di file e risolvere il problema:

- Visualizza la capacità massima di file del volume: per ulteriori informazioni, consulta Monitoraggio della capacità di file di un volume nella Guida per l'utente di Amazon FSx for NetApp ONTAP.
- Aumenta la capacità dei file del volume aumentando il numero di inode o aumentando la capacità di archiviazione. Per ulteriori informazioni, consulta Aumento della capacità massima di file di un volume nella Guida per l'utente di Amazon FSx for NetApp ONTAP.

Per determinare se il volume ha esaurito la capacità di storage disponibile e risolvere il problema:

- Determina la capacità di storage disponibile del volume: per ulteriori informazioni, consulta Monitoring Volume Storage Capacity nella Guida FSx per l'utente di for ONTAP.

  Se il volume ha poca o nessuna capacità di archiviazione disponibile, è necessario aumentare la capacità di archiviazione del volume. Per ulteriori informazioni, consulta Aumentare la capacità di archiviazione di un volume nella Guida FSx per l'utente di for ONTAP.
- Per evitare che il problema dell'esaurimento della capacità di archiviazione disponibile del volume si ripresenti, utilizza la funzionalità di ridimensionamento automatico del volume per aumentare automaticamente la capacità di archiviazione del volume in base alle esigenze. Per ulteriori informazioni, vedere Using Volume Autosizing nella Guida FSx per l'utente di for ONTAP.

Per determinare se l'esecuzione dell'operazione stava consumando una quantità eccessiva della capacità di throughput disponibile del file system:

- Monitora le prestazioni del file system utilizzando le CloudWatch metriche disponibili. Per ulteriori informazioni, consulta Monitoraggio delle metriche del file system nella Guida FSx per l'utente di for ONTAP.

- Monitora il file system per gli avvisi sulle prestazioni dei file server nella FSx console Amazon. Per ulteriori informazioni, consulta gli avvisi e i consigli sulle prestazioni nella Guida FSx per l'utente di for ONTAP.

Per risolvere il problema è necessario assicurarsi che l'operazione non utilizzi tutta la capacità di throughput disponibile del file system. Esegui questa operazione:

- Imposta il limite di larghezza di banda per l'esecuzione dell'attività su un valore inferiore alla capacità di FSx throughput fornita dal file system ONTAP. Per ulteriori informazioni, consulta the section called “Impostazione dei limiti di larghezza di banda”.
- In alternativa, è possibile aumentare la capacità di throughput assegnata al file system. Per ulteriori informazioni, vedere Aggiornamento della capacità di trasmissione nella Guida FSx per l'utente di for ONTAP.

L'operazione non riesce con **`Host is down`** un messaggio **`Connection Reset by peer`** FSx per il file system ONTAP

Se l' DataSync operazione non riesce con un `Host is down` messaggio `Connection Reset by peer` or durante il trasferimento di dati con un file system FSx for ONTAP, può essere dovuto a uno o più dei seguenti problemi.

- Il server SMB del file system è stato riavviato o altrimenti disconnesso durante l'esecuzione dell'operazione.
- Il file system ha eseguito il failover dal server primario a quello secondario (e all'indirizzo IP) durante l'esecuzione dell'operazione. DataSync non supporta il failover su un indirizzo IP secondario durante l'esecuzione dell'operazione.

  FSx per il failover dei file system ONTAP su un server e un indirizzo IP secondari durante i seguenti eventi:

  - Il server primario diventa non disponibile.
  - La zona di disponibilità del server primario diventa non disponibile (per i file system Multi-AZ).
  - Durante una modifica della capacità di throughput avviata dall'utente.
  - Durante la normale finestra di manutenzione programmata del file system.

  Per ulteriori informazioni, consulta FSx il processo di failover di ONTAP nella Guida FSx per l'utente di for ONTAP.

Operazioni da eseguire

Riavviare l'attività.

L'esecuzione dell'attività ha lo stato di avvio, ma sembra che non stia succedendo nulla

L' DataSync attività può rimanere bloccata con lo stato di avvio, in genere perché l'agente è spento o ha perso la connettività di rete.

Operazione da eseguire

Assicurati che lo stato del tuo agente sia ONLINE. Se l'agente è OFFLINE, assicurati che sia acceso.

Se l'agente è acceso e l'attività è ancora in corso, è probabile che si tratti di un problema di connessione di rete tra l'agente e AWS. Per informazioni su come testare la connettività di rete, consulta Verifica della connessione del tuo agente al servizio DataSync.

Se il problema persiste, consultaNon so cosa stia succedendo con il mio agente. Qualcuno può aiutarmi?.

L'esecuzione dell'attività sembra bloccata nello stato di preparazione

L'ora in cui l'operazione di DataSync trasferimento raggiunge lo stato Preparazione dipende dalla quantità di dati presenti nell'origine e nella destinazione del trasferimento e dalle prestazioni di tali sistemi di storage.

All'avvio di un'operazione, DataSync esegue un elenco ricorsivo delle directory per individuare tutti i file, gli oggetti, le directory e i metadati presenti nell'origine e nella destinazione. DataSync utilizza questi elenchi per identificare le differenze tra i sistemi di storage e determinare cosa copiare. Questo processo può richiedere alcuni minuti o anche alcune ore.

Operazione da eseguire

Non dovresti fare nulla. Continua ad attendere che lo stato dell'attività passi a Trasferimento. Se lo stato continua a non cambiare, contatta il Supporto AWS Centro.

L'esecuzione dell'attività si interrompe prima del termine del trasferimento

Se l'esecuzione dell' DataSync attività si interrompe in anticipo, è possibile Regione AWS che la configurazione dell'attività includa un elemento disabilitato nel file Account AWS.

Operazioni da eseguire

Effettua le seguenti operazioni per eseguire nuovamente l'attività:

1. Controlla lo stato di attivazione delle regioni dell'attività e assicurati che siano abilitate.
2. Riavvia l'attività.

L'esecuzione dell'attività non riesce durante il trasferimento da un bucket di Google Cloud Storage

Poiché DataSync comunica con Google Cloud Storage utilizzando l'API Amazon S3, esiste una limitazione che potrebbe causare DataSync il fallimento del trasferimento se provi a copiare i tag degli oggetti. Il seguente messaggio relativo al problema viene visualizzato nei tuoi CloudWatch log:

[AVVISO] Impossibile leggere i metadati per il file/*your-bucket*/*your-object*: S3 Get Object Tagging Failed: si procede senza applicare tag

Per evitare che ciò accada, deselezionate l'opzione Copia i tag degli oggetti durante la configurazione delle impostazioni dell'attività di trasferimento.

Vi sono discrepanze tra i timestamp di esecuzione dell'attività

Guardando la DataSync console o CloudWatch i log di Amazon, potresti notare che gli orari di inizio e fine dell'esecuzione delle DataSync attività non corrispondono ai timestamp che vedi in altri strumenti di monitoraggio. Questo perché la console e CloudWatch i log tengono conto del tempo impiegato dall'esecuzione di un'attività negli stati di avvio o di coda, a differenza di altri strumenti.

È possibile notare questa discrepanza quando si confrontano i timestamp di esecuzione tra la console o i registri e le seguenti posizioni: DataSync CloudWatch

- Registri del file system coinvolto nel trasferimento
- La data dell'ultima modifica su un oggetto Amazon S3 che ha DataSync scritto su
- Traffico di rete proveniente dall'agente DataSync
- EventBridge Eventi Amazon

L'esecuzione dell'attività fallisce con **`NoMem`** errori

Il set di dati che stai tentando di trasferire potrebbe essere troppo grande per DataSync. Se vedi questo errore, contatta Supporto AWS Center.

`user metadata key`Errore nel trasferimento dell'oggetto Azure Blob Storage

Durante il trasferimento da un bucket S3 aAzure Blob Storage, potresti visualizzare il seguente errore:

```
[ERROR] Failed to transfer file /user-metadata/file1: Azure Blob user metadata key must
 be a CSharp identifier
```

Ciò significa che */user-metadata/file1* include i metadati utente che non utilizzano un identificatore C# valido. Per ulteriori informazioni, consulta la documentazione di Microsoft.

C'è una **`/.aws-datasync`** cartella nella posizione di destinazione

DataSync crea una cartella denominata `/.aws-datasync` nella posizione di destinazione per facilitare il trasferimento dei dati.

Sebbene DataSync in genere elimini questa cartella dopo il trasferimento, potrebbero verificarsi situazioni in cui ciò non accade.

Operazione da eseguire

Elimina questa cartella in qualsiasi momento, purché non sia in esecuzione un'operazione che esegue la copia in quella posizione.

Non è possibile trasferire collegamenti simbolici tra sedi utilizzando SMB

Al termine dell'esecuzione dell'attività, viene visualizzato il seguente errore:

```
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.
```

Durante il trasferimento tra sistemi di storage SMB (ad esempio un file server SMB e il file system Amazon FSx for Windows File Server), potresti visualizzare i seguenti avvisi ed errori nei tuoi log: CloudWatch

```
[WARN] Failed to read metadata for file /appraiser/symlink: No data available
[ERROR] Failed to read metadata for directory /appraiser/symlink: No data available
```

Operazione da eseguire

DataSync non supporta il trasferimento di link simbolici (o hard link) durante il trasferimento tra questi tipi di posizione. Per ulteriori informazioni, consulta Collegamenti e directory copiati da AWS DataSync.

Errori nel report delle attività

È possibile che si verifichi uno dei seguenti errori durante il tentativo di monitorare il DataSync trasferimento con un rapporto sulle attività.

Messaggio di errore	Soluzione alternativa
Il percorso del file supera la lunghezza massima di 4.096 caratteri. Impossibile scrivere su Task Report	N/A (non è DataSync possibile trasferire un file con un percorso superiore a 4.096 byte) Per ulteriori informazioni, consulta Limiti del sistema di storage, dei file e degli oggetti.
Impossibile caricare i report delle attività su S3 a causa di un bucket o di un ruolo IAM non valido	Verifica che il ruolo DataSync IAM disponga delle autorizzazioni giuste per caricare un task report nel tuo bucket S3.
Si è verificato un errore di esecuzione prima della generazione di qualsiasi Task Report	Controlla i CloudWatch registri per identificare il motivo per cui l'esecuzione dell'attività non è riuscita.

Risoluzione dei problemi di verifica dei dati

Per impostazione predefinita, AWS DataSync verifica l'integrità dei dati al termine di un trasferimento. Utilizza le seguenti informazioni per aiutarti a diagnosticare gli errori e gli avvisi di verifica più comuni, come la modifica o l'eliminazione dei file prima del DataSync completamento della verifica dei dati.

In caso di problemi di verifica, molte volte è utile rivedere CloudWatch i registri (o rapporti sulle attività) oltre all'errore di esecuzione delle attività che riscontri. DataSyncfornisce log strutturati in JSON per le attività in modalità avanzata, mentre le attività in modalità Basic hanno registri non strutturati.

Vi sono delle discrepanze tra i contenuti di un file

Al termine dell'esecuzione dell'attività, viene visualizzato il seguente errore:

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

Nei CloudWatch registri, potresti notare che le verifiche non sono riuscite per i contenuti che differiscono tra le posizioni di origine e di destinazione. Questo può accadere se i file vengono modificati durante il trasferimento.

Ad esempio, i seguenti registri mostrano che `file1.txt` ha `dstHash` valori e diversi`mtime`: `srcHash`

Esempio di log in modalità base

```
[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 DataSync, `mtime` rappresenta l'ultima volta in cui è stato scritto un file prima della preparazione. Durante la verifica dei trasferimenti, DataSync confronta i `mtime` valori tra le posizioni di origine e di

destinazione. Un errore di verifica come questo si verifica se il file `mtime` per un file non è lo stesso per entrambe le posizioni. Le differenze tra `srcHash` e `dstHash` indicano che il contenuto del file non corrisponde in entrambe le posizioni.

Operazioni da eseguire

Esegui questa operazione:

1. Utilizzate un convertitore temporale per determinare se il file o l'oggetto di origine o di destinazione è stato modificato più di recente. Questo può aiutare a identificare la versione corrente.
2. Per evitare che si verifichi nuovamente questo errore, pianifica l'esecuzione dell'operazione durante una finestra di manutenzione quando non ci sono attività all'origine e alla destinazione.

C'è una mancata corrispondenza tra i metadati SMB di un file

Al termine dell'esecuzione dell'attività, viene visualizzato il seguente errore:

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

Durante il trasferimento tra sistemi di storage che supportano il protocollo Server Message Block (SMB), è possibile che venga visualizzato questo errore quando gli attributi SMB estesi di un file non corrispondono tra origine e destinazione.

Ad esempio, i registri seguenti mostrano che `file1.txt` ha un `extAttrsHash` valore diverso tra le posizioni, a indicare che il contenuto del file è identico ma gli attributi estesi non sono stati impostati nella destinazione:

Esempio di log in modalità base

```
[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
```

Potresti anche visualizzare un messaggio di errore correlato sugli attributi estesi:

```
[ERROR] Deferred error: WriteFileExtAttr2 failed to setextattrlist(filename="/
directory1/directory2/file1.txt"): Input/output error
```

Operazione da eseguire

Questo errore si verifica in genere quando le autorizzazioni per copiare gli elenchi di controllo di accesso (ACLs) nella destinazione sono insufficienti. Per risolvere questo problema, consulta le seguenti guide di configurazione in base al tipo di destinazione:

- Autorizzazioni richieste FSx per i file system Windows File Server
- Autorizzazioni richieste FSx per i file system ONTAP che utilizzano SMB

I file da trasferire non si trovano più nella posizione di origine

Al termine dell'esecuzione dell'attività, viene visualizzato il seguente errore:

```
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.
```

Nei registri, è possibile che vengano visualizzati errori che indicano che i file non si trovano nella posizione di origine. Questo può accadere se i file (come `file1.dll` `efile2.dll`) vengono eliminati dopo la preparazione ma prima del DataSync trasferimento:

Esempio di log in modalità base

```
[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
```

Operazione da eseguire

Per evitare queste situazioni, pianifica l'esecuzione dell'attività in assenza di attività nella posizione di origine.

Ad esempio, puoi eseguire l'attività durante una finestra di manutenzione quando gli utenti e le applicazioni non lavorano attivamente in quella posizione.

In alcuni casi, potresti non visualizzare i log associati a questo errore. In tal caso, contatta il Supporto AWS Centro.

DataSync non è possibile verificare i dati di destinazione

Al termine dell'esecuzione dell'attività, viene visualizzato il seguente errore:

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

Nei registri, potresti notare che non è DataSync possibile verificare determinate cartelle o file nella posizione di destinazione. Questi errori possono avere il seguente aspetto:

Esempio di log in modalità base

```
[ERROR] Failed to read metadata for destination file /directory1/directory2/
file1.txt: No such file or directory
```

Per quanto riguarda i file, potresti riscontrare errori di verifica come questi:

Esempio di registro in modalità base

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt   srcMeta: type=R mode=0755 uid=65534
 gid=65534 size=61533 atime=1633099987/747713800 mtime=1536995631/894267700
 extAttrsHash=232104771
[NOTICE]   srcHash: 1426fe40f669a7d36cca1b5329983df31a9aeff8eb9fe3ac885f26de2f8fff6b
[NOTICE] /directory1/directory2/file1.txt   dstMeta: type=R mode=0755 uid=65534
 gid=65534 size=0 atime=0/0 mtime=0/0 extAttrsHash=0
[NOTICE]   dstHash: 0000000000000000000000000000000000000000000000000000000000000000
```

Operazione da eseguire

Questi registri indicano che i dati di destinazione sono stati eliminati dopo il trasferimento ma prima della verifica. (I log hanno un aspetto simile quando i dati vengono caricati in una posizione di origine nello stesso periodo di tempo.)

Per evitare queste situazioni, pianifica l'esecuzione dell'attività in assenza di attività nella località di destinazione.

Ad esempio, puoi eseguire l'attività durante una finestra di manutenzione quando gli utenti e le applicazioni non lavorano attivamente in quella posizione.

DataSync non è in grado di leggere i metadati degli oggetti

Al termine dell'esecuzione dell'attività, viene visualizzato il seguente errore:

```
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.
```

Nei tuoi log, potresti notare che non è DataSync possibile leggere a `file1.png` causa di una richiesta Amazon `HeadObject` S3 non riuscita. DataSync effettua `HeadObject` richieste presso le sedi S3 durante la preparazione e la verifica delle attività.

Esempio di log in modalità base

```
[WARN] Failed to read metadata for file /file1.png: S3 Head Object Failed
```

Operazioni da eseguire

Per risolvere questo problema, verifica se DataSync disponi del giusto livello di autorizzazioni per lavorare con il tuo bucket S3:

- Assicurati che il ruolo IAM DataSync utilizzato per accedere alle tue sedi Amazon S3 consenta l'`s3:GetObject`autorizzazione. Per ulteriori informazioni, consulta Autorizzazioni richieste.
- Se il tuo bucket S3 utilizza la crittografia lato server, assicurati che DataSync sia autorizzato ad accedere agli oggetti in quel bucket. Per ulteriori informazioni, consulta Accesso ai bucket S3 utilizzando la crittografia lato server.

C'è una mancata corrispondenza nei metadati definiti dal sistema di un oggetto

Al termine dell'esecuzione dell'attività in modalità avanzata tra i bucket S3, viene visualizzato il seguente errore:

```
Verification failed due to a difference in metadata
```

Potresti notare nei tuoi log una mancata corrispondenza nei metadati definiti dal sistema Amazon S3 di un oggetto. In questo esempio particolare, l'oggetto di origine non ha `Content-Type` metadati, mentre l'oggetto di destinazione sì. Ciò è accaduto perché il bucket S3 di destinazione applicava automaticamente `"ContentType": "application/octet-stream"` i metadati all'oggetto quando DataSync lo trasferiva lì.

Esempio di registro in modalità avanzata


```
{
    "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"
}
```

Operazione da eseguire

Per evitare questo errore, aggiorna gli oggetti di posizione di origine in modo da includere la proprietà `Content-Type` dei metadati.

Comprensione della durata della verifica dei dati

DataSync la verifica include un SHA256 checksum sul contenuto dei file e un confronto esatto dei metadati dei file tra le posizioni. La durata della verifica dipende da diversi fattori, tra cui il numero di file o oggetti coinvolti, la dimensione dei dati nei sistemi di storage e le prestazioni di questi sistemi.

Operazione da eseguire

Dati i fattori che possono influire sui tempi di verifica, non dovresti fare nulla. Tuttavia, se l'esecuzione dell'attività sembra bloccata con uno stato di verifica, contatta il Supporto AWS Centro.

Risoluzione dei problemi relativi ai costi di storage S3 superiori al previsto con DataSync

Se i costi di storage di Amazon S3 sono più elevati di quanto pensavi a seguito di un AWS DataSync trasferimento, ciò potrebbe essere dovuto a uno o più dei seguenti motivi:

- Quando effettui il trasferimento da o verso i bucket S3, devi sostenere dei costi relativi alle richieste API S3 effettuate da. DataSync
- DataSync utilizza la funzionalità di caricamento multiparte di Amazon S3 per caricare oggetti nei bucket S3. Questo approccio può comportare costi di archiviazione imprevisti per i caricamenti che non vengono completati correttamente.
- Nel bucket S3 potrebbe essere attiva la funzione Versioni multiple degli oggetti. Il controllo delle versioni degli oggetti fa sì che Amazon S3 memorizzi più copie di oggetti con lo stesso nome.

Operazioni da eseguire

In questi casi, procedi come indicato di seguito:

- Assicurati di comprendere come DataSync utilizza le richieste S3 e in che modo potrebbero influire sui costi di storage. Per ulteriori informazioni, consulta Valutazione dei costi delle richieste S3 durante l'utilizzo DataSync.
- Se il problema riguarda i caricamenti in più parti, configura una politica per i caricamenti multiparte per il tuo bucket S3 per eliminare i caricamenti multiparte incompleti e ridurre i costi di archiviazione. Per ulteriori informazioni, consulta il post AWS sul blog S3 Lifecycle Management Update - Support for Multipart Uploads and Delete Markers.
- Se il problema riguarda il controllo delle versioni degli oggetti, disabilita il controllo delle versioni degli oggetti sul tuo bucket S3.
- Se hai bisogno di ulteriore assistenza, contatta Center.Supporto AWS

AWS DataSync tutorial

Questi tutorial ti guidano attraverso alcuni scenari del mondo reale con. AWS DataSync

Argomenti

- Tutorial: trasferimento di dati dallo storage locale ad Amazon S3 attraverso Account AWS
- Tutorial: trasferimento di dati tra bucket Amazon S3 attraverso Account AWS

Tutorial: trasferimento di dati dallo storage locale ad Amazon S3 attraverso Account AWS

Quando si utilizza AWS DataSync con l'archiviazione locale, in genere si trasferiscono i dati a un servizio di AWS archiviazione che appartiene allo Account AWS stesso agente. DataSync In alcune situazioni, tuttavia, potrebbe essere necessario trasferire dati in un bucket Amazon S3 associato a un account diverso.

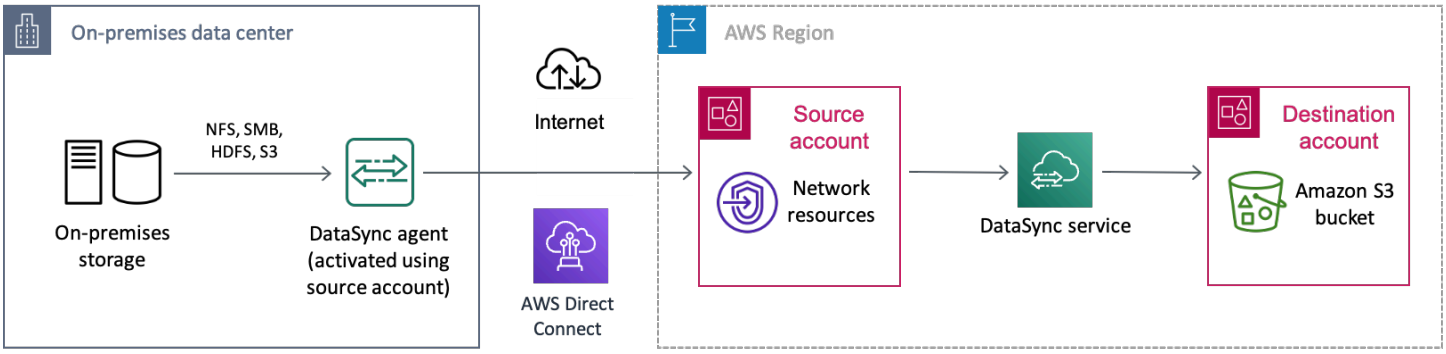
> **Important**
>
> Il trasferimento di dati Account AWS tramite i metodi descritti in questo tutorial funziona solo quando Amazon S3 è una delle sedi di DataSync trasferimento.

Panoramica

Non è raro dover trasferire dati tra diversi paesi Account AWS, soprattutto se si dispone di team separati che gestiscono le risorse dell'organizzazione. Ecco come DataSync può apparire un trasferimento tra account diversi:

- Account di origine: utilizzato Account AWS per la gestione delle risorse di rete. Questo è l'account con cui attivi il tuo DataSync agente.
- Account di destinazione: Account AWS per la gestione del bucket S3 a cui devi trasferire i dati.

Il diagramma seguente illustra questo tipo di scenario.



Prerequisito: autorizzazioni richieste per l'account di origine

Per quanto riguarda la fonte Account AWS, ci sono due tipi di autorizzazioni da prendere in considerazione per questo tipo di trasferimento tra account:

- Autorizzazioni utente che consentono a un utente di lavorare con DataSync (potrebbe trattarsi dell'utente o dell'amministratore dello storage). Queste autorizzazioni consentono di creare DataSync posizioni e attività.
- DataSync autorizzazioni di servizio che consentono di DataSync trasferire dati nel bucket dell'account di destinazione.

User permissions

Nel tuo account di origine, aggiungi almeno le seguenti autorizzazioni a un ruolo IAM per la creazione di DataSync sedi e attività. Per informazioni su come aggiungere autorizzazioni a un ruolo, consulta la sezione Creazione o modifica di un ruolo IAM.

```
{
    "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",
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:AttachRolePolicy",
                "iam:ListRoles",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

> **Tip**
>
> Per configurare le autorizzazioni utente, valuta la possibilità di utilizzare. AWSDataSyncFullAccess Si tratta di una politica AWS gestita che fornisce all'utente l'accesso completo DataSync e un accesso minimo alle sue dipendenze.

DataSync service permissions

Il DataSync servizio richiede le seguenti autorizzazioni nell'account di origine per trasferire i dati nel bucket di account di destinazione.

Più avanti in questo tutorial, aggiungerai queste autorizzazioni durante la creazione di un ruolo IAM per. DataSync Specificate questo ruolo (*source-datasync-role*) anche nella vostra policy sul bucket di destinazione e durante la creazione della posizione di DataSync destinazione.

```
{
  "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/*"
    }
  ]
}
```

Prerequisito: autorizzazioni richieste per l'account di destinazione

Nel tuo account di destinazione, le autorizzazioni utente devono consentirti di aggiornare la politica del bucket di destinazione e disabilitarne gli elenchi di controllo degli accessi (). ACLs Per ulteriori informazioni su queste autorizzazioni specifiche, consulta la Amazon S3 User Guide.

Passaggio 1: nel tuo account di origine, crea un agente DataSync

Per iniziare, è necessario creare un DataSync agente in grado di leggere dal sistema di storage locale e comunicare con il DataSync servizio. Questo processo include la distribuzione di un agente nell'ambiente di storage locale e l'attivazione dell'agente nell'origine. Account AWS

> **Note**
>
> I passaggi di questo tutorial si applicano a qualsiasi tipo di agente e endpoint di servizio utilizzato.

Per creare un agente DataSync

1. Implementa un DataSync agente nel tuo ambiente di storage locale.
2. Scegli un endpoint di servizio con cui l'agente utilizzerà per comunicare. AWS
3. Attiva il tuo agente nel tuo account di origine.

Passaggio 2: nel tuo account di origine, crea un ruolo DataSync IAM per l'accesso al bucket di destinazione

Nel tuo account di origine, hai bisogno di un ruolo IAM che fornisca DataSync le autorizzazioni per trasferire i dati nel bucket di account di destinazione.

Poiché stai effettuando il trasferimento tra account, devi creare il ruolo manualmente. (DataSyncpuò creare questo ruolo per te nella console quando effettui il trasferimento nello stesso account.)

Crea il ruolo DataSync IAM

Crea un ruolo IAM con DataSync come entità affidabile.

Per creare il ruolo IAM

1. Accedi al AWS Management Console con il tuo account di origine.
2. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
3. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli, quindi scegli Crea ruolo.
4. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli Servizio AWS.

5. Per Caso d'uso, scegli DataSyncnell'elenco a discesa e seleziona DataSync. Scegli Next (Successivo).
6. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
7. Dai un nome al tuo ruolo e scegli Crea ruolo.

Per ulteriori informazioni, consulta Creating a role for an Servizio AWS (console) nella IAM User Guide.

Aggiungi le autorizzazioni al ruolo DataSync IAM

Il ruolo IAM che hai appena creato necessita delle autorizzazioni che consentono di trasferire i dati DataSync al bucket S3 nel tuo account di destinazione.

Per aggiungere autorizzazioni al tuo ruolo IAM

1. Nella pagina Ruoli della console IAM, cerca il ruolo che hai appena creato e scegline il nome.
2. Nella pagina dei dettagli del ruolo, scegli la scheda Autorizzazioni. Scegli Aggiungi autorizzazioni, quindi Crea politica in linea.
3. Scegli la scheda JSON ed esegui le seguenti operazioni:

    a. Incolla il seguente codice JSON nell'editor delle politiche:

> **Note**
>
> Il valore per `aws:ResourceAccount` deve essere l'ID dell'account proprietario del bucket Amazon S3 specificato nella policy.

```
{
 "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. Sostituisci ogni istanza di *amzn-s3-demo-destination-bucket* con il nome del bucket S3 nel tuo account di destinazione.

4. Scegli Next (Successivo). Dai un nome alla tua politica e scegli Crea politica.

Passaggio 3: nell'account di destinazione, aggiorna la policy sui bucket S3

Nel tuo account di destinazione, modifica la policy del bucket S3 di destinazione per includere il ruolo DataSync IAM che hai creato nell'account di origine.

Prima di iniziare: assicurati di disporre delle autorizzazioni necessarie per l'account di destinazione.

Per aggiornare la policy del bucket S3 di destinazione

1. Nel AWS Management Console, passa all'account di destinazione.
2. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
3. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
4. Nell'elenco dei bucket, scegli il bucket S3 a cui stai trasferendo i dati.
5. Nella pagina dei dettagli del bucket, scegli la scheda Autorizzazioni.
6. In Bucket policy, scegli Modifica e procedi come segue per modificare la tua policy sui bucket S3:

   a. Aggiorna il contenuto dell'editor per includere le seguenti dichiarazioni politiche:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-account: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. Sostituisci ogni istanza di *source-account* con l' Account AWS ID del tuo account di origine.

c. Sostituiscilo *source-datasync-role* con il ruolo IAM per cui hai creato DataSync nel tuo account di origine.

d. Sostituisci ogni istanza di *amzn-s3-demo-destination-bucket* con il nome del bucket S3 nel tuo account di destinazione.

7. Scegli Save changes (Salva modifiche).

Passaggio 4: Nell'account di destinazione, disattivalo ACLs per il tuo bucket S3

È importante che tutti i dati che copi nel bucket S3 appartengano al tuo account di destinazione. Per garantire che questo account sia proprietario dei dati, disabilita gli elenchi di controllo degli accessi del bucket (). ACLs Per ulteriori informazioni, consulta la sezione Controllo della proprietà degli oggetti e disattivazione ACLs del bucket nella Amazon S3 User Guide.

Da disabilitare per il bucket ACLs di destinazione

1. Mentre sei ancora connesso alla console S3 con il tuo account di destinazione, scegli il bucket S3 su cui stai trasferendo i dati.
2. Nella pagina dei dettagli del bucket, scegli la scheda Autorizzazioni.
3. Alla voce Proprietà Oggetto scegli Modifica.
4. Se non è già selezionata, scegli l'opzione ACLs disabilitata (consigliata).
5. Scegli Save changes (Salva modifiche).

Passaggio 5: Nel tuo account di origine, crea una posizione di DataSync origine per lo storage locale

Nel tuo account di origine, crea una posizione di DataSync origine per il sistema di archiviazione locale da cui stai trasferendo i dati. Questa posizione utilizza l'agente che hai attivato nel tuo account di origine.

Passaggio 6: nel tuo account di origine, crea una posizione di DataSync destinazione per il tuo bucket S3

Mentre sei ancora nel tuo account di origine, crea una posizione per il bucket S3 su cui stai trasferendo i dati.

Prima di iniziare: assicurati di disporre delle autorizzazioni necessarie per il tuo account di origine.

Poiché non puoi creare posizioni tra account utilizzando l'interfaccia della DataSync console, queste istruzioni richiedono l'esecuzione di un `create-location-s3` comando per creare la posizione di destinazione. Ti consigliamo di eseguire il comando utilizzando AWS CloudShell una shell preautenticata basata su browser che puoi avviare direttamente dalla console. CloudShell consente di eseguire AWS CLI comandi `create-location-s3` senza scaricare o installare strumenti da riga di comando.

> **Note**
>
> Per completare i seguenti passaggi utilizzando uno strumento da riga di comando diverso da CloudShell, assicurati che il tuo AWS CLI profilo utilizzi lo stesso ruolo IAM che include le autorizzazioni utente richieste da utilizzare DataSync nel tuo account di origine.

Per creare una posizione di DataSync destinazione utilizzando CloudShell

1. Mentre sei ancora nel tuo account di origine, esegui una delle seguenti operazioni per eseguire l'avvio CloudShell dalla console:
   - Scegli l' CloudShell icona nella barra di navigazione della console. Si trova alla destra della casella di ricerca.
   - Utilizza la casella di ricerca sulla barra di navigazione della console per CloudShellcercare, quindi scegli l'CloudShellopzione.
2. Copia il seguente comando:

```
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. Sostituiscilo *amzn-s3-demo-destination-bucket* con il nome del bucket S3 nell'account di destinazione.
4. *source-user-account*Sostituiscilo con l' Account AWS ID del tuo account di origine.
5. Sostituiscilo *source-datasync-role* con il ruolo DataSync IAM che hai creato nel tuo account di origine.
6. Esegui il comando in CloudShell.

   Se il comando restituisce un ARN di DataSync posizione simile a questo, la posizione è stata creata con successo:

   ```
   {
     "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
   abcdef01234567890"
   }
   ```

7. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.

Dal tuo account di origine, puoi vedere la posizione S3 che hai appena creato per il bucket dell'account di destinazione.

Passaggio 7: Nel tuo account di origine, crea e avvia l'attività DataSync

Prima di iniziare un' DataSync attività di trasferimento dei dati, ricapitoliamo ciò che hai fatto finora:

- Nel tuo account di origine, hai creato il tuo DataSync agente. L'agente può leggere dal sistema di storage locale e comunicare con il DataSync servizio.
- Nel tuo account di origine, hai creato un ruolo IAM che consente di DataSync trasferire i dati al bucket S3 dell'account di destinazione.
- Nel tuo account di destinazione, hai configurato il bucket S3 in modo che DataSync possa trasferirvi i dati.
- Nel tuo account di origine, hai creato le posizioni di DataSync origine e di destinazione per il trasferimento.

Per creare e avviare l' DataSync operazione

1. Mentre usi ancora la DataSync console nel tuo account di origine, espandi Trasferimento dati nel riquadro di navigazione a sinistra, quindi scegli Attività e Crea attività.

2. Nella pagina Configura la posizione di origine, scegli Scegli una posizione esistente. Scegli la posizione di origine da cui stai copiando i dati (l'archiviazione locale), quindi Avanti.
3. Nella pagina Configura posizione di destinazione, scegli Scegli una posizione esistente. Scegli la posizione di destinazione in cui stai copiando i dati (il bucket S3 nel tuo account di destinazione), quindi Avanti.
4. Nella pagina Configura impostazioni, assegna un nome all'attività. Se necessario, configura impostazioni aggiuntive, come specificare un gruppo di CloudWatch log Amazon. Scegli Next (Successivo).
5. Nella pagina Revisione, rivedi le impostazioni e scegli Crea attività.
6. Nella pagina dei dettagli dell'attività, scegli Avvia, quindi scegli una delle seguenti opzioni:
   - Per eseguire l'attività senza modifiche, scegli Inizia con i valori predefiniti.
   - Per modificare l'attività prima di eseguirla, scegli Inizia con opzioni di sovrascrittura.

Al termine dell'attività, controlla il bucket S3 nel tuo account di destinazione. Dovresti vedere i dati che sono stati trasferiti dalla tua posizione di origine.

Risorse correlate

Per ulteriori informazioni su ciò che hai fatto in questo tutorial, consulta i seguenti argomenti:

- Creare un ruolo per una Servizio AWS (console)
- Modifica di una politica di attendibilità dei ruoli (console)
- Aggiungere una policy sui bucket utilizzando la console Amazon S3
- Crea una posizione S3 con AWS CLI

Tutorial: trasferimento di dati tra bucket Amazon S3 attraverso Account AWS

Con AWS DataSync, puoi trasferire dati tra bucket Amazon S3 che appartengono a diversi. Account AWS

> **Important**
>
> Il trasferimento di dati Account AWS tramite i metodi descritti in questo tutorial funziona solo con Amazon S3. Inoltre, questo tutorial può aiutarti a trasferire dati tra bucket S3, anch'essi in diversi formati. Regioni AWS

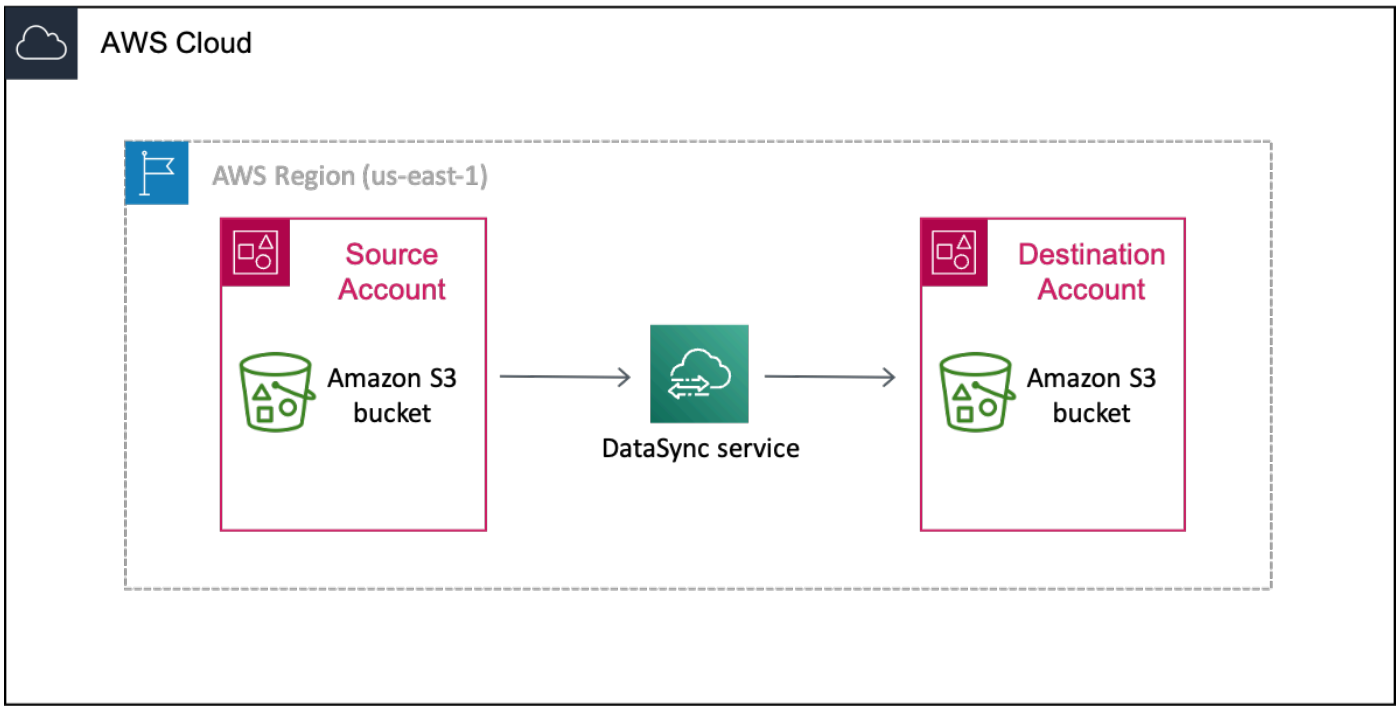
Panoramica

Non è raro trasferire dati da un paese all'altro Account AWS, soprattutto se avete team separati che gestiscono le risorse dell'organizzazione. Ecco come DataSync può essere eseguito un trasferimento tra account diversi:

- Account di origine: Account AWS per la gestione del bucket S3 da cui devi trasferire i dati.
- Account di destinazione: Account AWS per la gestione del bucket S3 a cui devi trasferire i dati.

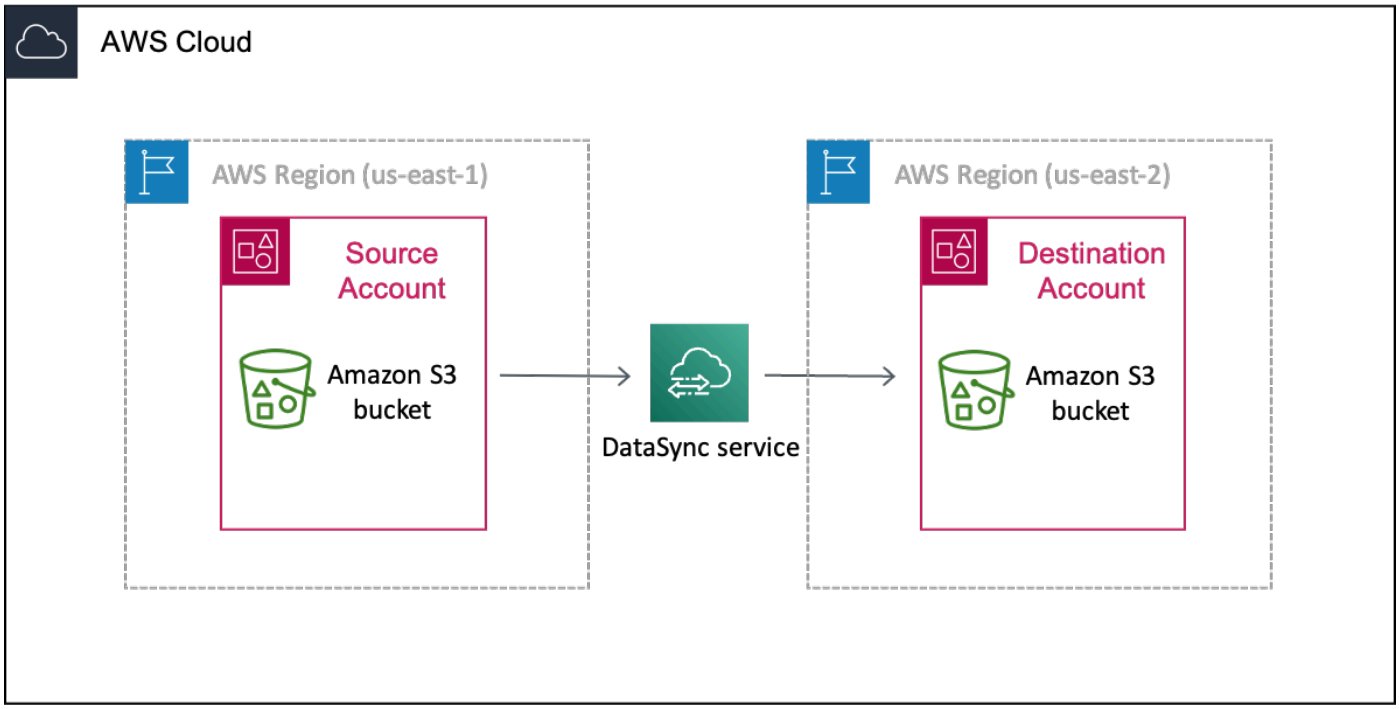
Transfers across accounts

Il diagramma seguente illustra uno scenario in cui si trasferiscono dati da un bucket S3 a un altro bucket S3 che si trova in un altro bucket S3. Account AWS



Transfers across accounts and Regions

Il diagramma seguente illustra uno scenario in cui si trasferiscono dati da un bucket S3 a un altro bucket S3 che si trova in una regione e diversa. Account AWS



Prerequisito: autorizzazioni richieste per l'account di origine

Per quanto riguarda la fonte Account AWS, ci sono due tipi di autorizzazioni da prendere in considerazione per questo tipo di trasferimento tra account:

- Autorizzazioni utente che consentono a un utente di lavorare con DataSync (potrebbe trattarsi dell'utente o dell'amministratore dello storage). Queste autorizzazioni consentono di creare DataSync posizioni e attività.
- DataSync autorizzazioni di servizio che consentono di DataSync trasferire dati nel bucket dell'account di destinazione.

Autorizzazioni utente per il tuo account di origine

Nel tuo account di origine, aggiungi almeno le seguenti autorizzazioni a un ruolo IAM per la creazione di DataSync sedi e attività. Per informazioni su come aggiungere autorizzazioni a un ruolo, consulta la sezione Creazione o modifica di un ruolo IAM.

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",
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:AttachRolePolicy",
                "iam:ListRoles",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
            }
        }
    ]
```

```
}
```

> **Tip**
>
> Per configurare le autorizzazioni utente, valuta la possibilità di utilizzare. AWSDataSyncFullAccess Si tratta di una politica AWS gestita che fornisce all'utente l'accesso completo DataSync e un accesso minimo alle sue dipendenze.

DataSync autorizzazioni di servizio per l'account di origine

Il DataSync servizio richiede le seguenti autorizzazioni nell'account di origine per trasferire i dati nel bucket dell'account di destinazione.

Più avanti in questo tutorial, aggiungerai queste autorizzazioni durante la creazione di un ruolo IAM per. DataSync Specificate questo ruolo (*source-datasync-role*) anche nella vostra policy sul bucket di destinazione e durante la creazione della posizione di DataSync destinazione.

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/*"
    }
  ]
}
```

Prerequisito: autorizzazioni richieste per l'account di destinazione

Nel tuo account di destinazione, le autorizzazioni utente devono consentirti di aggiornare la politica del bucket di destinazione e disabilitarne gli elenchi di controllo degli accessi (). ACLs Per ulteriori informazioni su queste autorizzazioni specifiche, consulta la Amazon S3 User Guide.

Passaggio 1: nel tuo account di origine, crea un ruolo DataSync IAM per l'accesso al bucket di destinazione

Nella tua fonte Account AWS, hai bisogno di un ruolo IAM che fornisca DataSync le autorizzazioni per trasferire i dati nel bucket di account di destinazione.

Poiché stai effettuando il trasferimento tra account, devi creare il ruolo manualmente. (DataSyncpuò creare questo ruolo per te nella console quando effettui il trasferimento nello stesso account.)

Crea il ruolo DataSync IAM

Crea un ruolo IAM con DataSync come entità affidabile.

1. Accedi al AWS Management Console con il tuo account di origine.
2. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
3. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli, quindi scegli Crea ruolo.
4. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli Servizio AWS.
5. Per Caso d'uso, scegli DataSyncnell'elenco a discesa e seleziona DataSync. Scegli Next (Successivo).
6. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
7. Dai un nome al tuo ruolo e scegli Crea ruolo.

Per ulteriori informazioni, consulta Creating a role for an Servizio AWS (console) nella IAM User Guide.

Aggiungi le autorizzazioni al ruolo DataSync IAM

Il ruolo IAM che hai appena creato necessita delle autorizzazioni che consentono di trasferire i dati DataSync al bucket S3 nel tuo account di destinazione.

1. Nella pagina Ruoli della console IAM, cerca il ruolo che hai appena creato e scegline il nome.
2. Nella pagina dei dettagli del ruolo, scegli la scheda Autorizzazioni. Scegli Aggiungi autorizzazioni, quindi Crea politica in linea.
3. Scegli la scheda JSON ed esegui le seguenti operazioni:

   a. Incolla il seguente codice JSON nell'editor delle politiche:

> **Note**
>
> Il valore per `aws:ResourceAccount` deve essere l'ID dell'account proprietario del bucket Amazon S3 specificato nella policy.

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. Sostituisci ogni istanza di *amzn-s3-demo-destination-bucket* con il nome del bucket S3 nel tuo account di destinazione.

4. Scegli Next (Successivo). Dai un nome alla tua politica e scegli Crea politica.

Passaggio 2: nell'account di destinazione, aggiorna la policy sui bucket S3

Nel tuo account di destinazione, modifica la policy del bucket S3 di destinazione per includere il ruolo DataSync IAM che hai creato nell'account di origine.

Prima di iniziare: assicurati di disporre delle autorizzazioni necessarie per l'account di destinazione.

Aggiorna la policy sui bucket S3 di destinazione

1. Nel AWS Management Console, passa all'account di destinazione.
2. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
3. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
4. Nell'elenco dei bucket, scegli il bucket S3 a cui stai trasferendo i dati.

5. Nella pagina dei dettagli del bucket, scegli la scheda Autorizzazioni.
6. In Bucket policy, scegli Modifica e procedi come segue per modificare la tua policy sui bucket S3:

   a. Aggiorna il contenuto dell'editor per includere le seguenti dichiarazioni politiche:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-account: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. Sostituisci ogni istanza di *source-account* con l' Account AWS ID del tuo account di origine.

   c. Sostituiscilo *source-datasync-role* con il ruolo IAM per cui hai creato DataSync nel tuo account di origine.

   d. Sostituisci ogni istanza di *amzn-s3-demo-destination-bucket* con il nome del bucket S3 nel tuo account di destinazione.

7. Scegli Save changes (Salva modifiche).

Passaggio 3: nell'account di destinazione, disattivalo ACLs per il tuo bucket S3

È importante che tutti i dati che trasferisci nel bucket S3 appartengano al tuo account di destinazione. Per garantire che questo account sia proprietario dei dati, disabilita gli elenchi di controllo degli accessi del bucket (). ACLs Per ulteriori informazioni, consulta la sezione Controllo della proprietà degli oggetti e disattivazione ACLs del bucket nella Amazon S3 User Guide.

Prima di iniziare: assicurati di disporre delle autorizzazioni necessarie per l'account di destinazione.

Disattiva il bucket S3 di destinazione ACLs

1. Mentre sei ancora connesso alla console S3 con il tuo account di destinazione, scegli il bucket S3 su cui stai trasferendo i dati.
2. Nella pagina dei dettagli del bucket, scegli la scheda Autorizzazioni.
3. Alla voce Proprietà Oggetto scegli Modifica.
4. Se non è già selezionata, scegli l'opzione ACLs disabilitata (consigliata).
5. Scegli Save changes (Salva modifiche).

Passaggio 4: Nel tuo account di origine, crea le tue DataSync sedi

Nel tuo account di origine, crea le DataSync posizioni per i bucket S3 di origine e di destinazione.

Prima di iniziare: assicurati di disporre delle autorizzazioni necessarie per il tuo account di origine.

Crea la tua posizione DataSync di origine

- Nel tuo account di origine, crea una posizione per il bucket S3 da cui stai trasferendo i dati.

Crea la tua località di destinazione DataSync

Mentre sei ancora nel tuo account di origine, crea una posizione per il bucket S3 su cui stai trasferendo i dati.

Poiché non puoi creare posizioni tra più account utilizzando l'interfaccia della DataSync console, queste istruzioni richiedono l'esecuzione di un `create-location-s3` comando per creare la posizione di destinazione. Ti consigliamo di eseguire il comando utilizzando AWS CloudShell una shell preautenticata basata su browser che puoi avviare direttamente dalla console.

CloudShellconsente di eseguire AWS CLI comandi `create-location-s3` senza scaricare o installare strumenti da riga di comando.

> **Note**
>
> Per completare i seguenti passaggi utilizzando uno strumento da riga di comando diverso da CloudShell, assicurati che il tuo AWS CLI profilo utilizzi lo stesso ruolo IAM che include le autorizzazioni utente richieste da utilizzare DataSync nel tuo account di origine.

Per creare una posizione di DataSync destinazione utilizzando CloudShell

1. Mentre sei ancora nel tuo account di origine, esegui una delle seguenti operazioni per eseguire l'avvio CloudShell dalla console:
   - Scegli l' CloudShell icona nella barra di navigazione della console. Si trova alla destra della casella di ricerca.
   - Utilizza la casella di ricerca sulla barra di navigazione della console per CloudShellcercare, quindi scegli l'CloudShellopzione.
2. Copia il seguente `create-location-s3` comando:

```
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. Sostituiscilo *amzn-s3-demo-destination-bucket* con il nome del bucket S3 nell'account di destinazione.
4. Se il bucket di destinazione si trova in una regione diversa da quella del bucket di origine, sostituiscilo *amzn-s3-demo-destination-bucket-region* con la regione in cui risiede il bucket di destinazione (ad esempio,). *us-east-2* Rimuovi questa opzione se i tuoi bucket si trovano nella stessa regione.
5. Sostituisci *source-account-id* con l' Account AWS ID di origine.
6. Sostituiscilo *source-datasync-role* con il ruolo DataSync IAM che hai creato nel tuo account di origine.

7. Esegui il comando in CloudShell.

   Se il comando restituisce un ARN di DataSync posizione simile a questo, la posizione è stata creata con successo:

   ```
   {
     "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
   abcdef01234567890"
   }
   ```

8. Nel riquadro di navigazione a sinistra, espandi Trasferimento dati, quindi scegli Posizioni.
9. Se hai creato la posizione in una regione diversa, scegli quella regione nel riquadro di navigazione.

Dal tuo account di origine, puoi vedere la posizione S3 che hai appena creato per il bucket dell'account di destinazione.

Passaggio 5: Nel tuo account di origine, crea e avvia l'attività DataSync

Prima di iniziare un' DataSync attività di trasferimento dei dati, ricapitoliamo ciò che hai fatto finora:

- Nel tuo account di origine, hai creato un ruolo IAM che consente di DataSync trasferire i dati nel bucket S3 dell'account di destinazione.
- Nel tuo account di destinazione, hai configurato il bucket S3 in modo che DataSync possa trasferirvi i dati.
- Nel tuo account di origine, hai creato le posizioni di DataSync origine e di destinazione per il trasferimento.

Crea e avvia la tua DataSync attività

1. Mentre usi ancora la DataSync console nel tuo account di origine, espandi Trasferimento dati nel riquadro di navigazione a sinistra, quindi scegli Attività e Crea attività.
2. Se il bucket nel tuo account di destinazione si trova in una regione diversa da quella del tuo account di origine, scegli la regione del bucket di destinazione nel pannello di navigazione in alto.

> **Important**
>
> Per evitare un errore di connessione di rete, devi creare l' DataSyncattività nella stessa regione della posizione di destinazione.

3. Nella pagina Configura la posizione di origine, procedi come segue:
   a. Seleziona Scegli una posizione esistente.
   b. (Per i trasferimenti tra regioni) Nel menu a discesa Regione, scegli la regione in cui risiede il bucket di origine.
   c. Per le sedi esistenti, scegli la posizione di origine per il bucket S3 da cui stai trasferendo i dati, quindi scegli Avanti.
4. Nella pagina Configura la posizione di destinazione, procedi come segue:
   a. Seleziona Scegli una posizione esistente.
   b. Per Posizioni esistenti, scegli la posizione di destinazione per il bucket S3 in cui stai trasferendo i dati, quindi scegli Avanti.
5. Nella pagina Configura impostazioni, scegli una modalità Attività.

> **Tip**
>
> Ti consigliamo di utilizzare la modalità Avanzata. Per ulteriori informazioni, consulta Scelta di una modalità di operazione per il trasferimento dei dati.

6. Assegna un nome all'attività e configura impostazioni aggiuntive, come specificare un gruppo di CloudWatch log Amazon. Scegli Next (Successivo).
7. Nella pagina Revisione, rivedi le impostazioni e scegli Crea attività.
8. Nella pagina dei dettagli dell'attività, scegli Avvia, quindi scegli una delle seguenti opzioni:
   - Per eseguire l'attività senza modifiche, scegli Inizia con i valori predefiniti.
   - Per modificare l'attività prima di eseguirla, scegli Inizia con opzioni di sovrascrittura.

Al termine dell'attività, controlla il bucket S3 nel tuo account di destinazione. Dovresti vedere i dati che sono stati spostati dal bucket dell'account di origine.

Risoluzione dei problemi

Fai riferimento alle seguenti informazioni se riscontri problemi nel tentativo di completare il trasferimento tra account.

Errori di connessione

Durante il trasferimento tra bucket S3 in diverse Account AWS aree geografiche con attività in modalità Base, è possibile che si verifichi un errore di connessione di rete all'avvio dell'operazione. DataSync Per risolvere questo problema, utilizza un'attività in modalità avanzata. In alternativa, crea un'attività in modalità Base nella stessa regione della posizione di destinazione e prova a eseguirla.

Correlata: Trasferimenti tra account con bucket S3 utilizzando la crittografia lato server

Se stai cercando di eseguire questo trasferimento con bucket S3 utilizzando la crittografia lato server, consulta lo Storage Blog per istruzioni.AWS

Esecuzione di una migrazione di dati di grandi dimensioni con AWS DataSync

Le migrazioni di dati su larga scala possono comportare il trasferimento di volumi significativi di dati che comprendono milioni di file o oggetti in vari formati. AWS DataSync semplifica questi trasferimenti complessi gestendo la pianificazione, il monitoraggio, la crittografia e la verifica dei dati.

Cos'è una migrazione di dati di grandi dimensioni?

Una migrazione di dati di grandi dimensioni comporta in genere il trasferimento di terabyte o più di dati distribuiti tra varie fonti verso un nuovo ambiente di storage di destinazione (in questo caso,). AWS Queste migrazioni richiedono una pianificazione e un coordinamento accurati all'interno dell'organizzazione per spostare i dati con successo e ridurre al minimo le interruzioni delle attività aziendali.

DataSync possono semplificare queste migrazioni, che di solito sono di natura complessa. Alcuni vantaggi dell'utilizzo DataSync per la migrazione includono:

- Gestione automatizzata dei processi di trasferimento dei dati e dell'infrastruttura necessaria per trasferimenti di dati sicuri e ad alte prestazioni.
- End-to-end sicurezza, inclusa la crittografia e la convalida dell'integrità dei dati, per garantire che i dati arrivino in modo sicuro, intatto e pronto all'uso.
- Un protocollo di rete appositamente progettato e un'architettura parallela multithread per accelerare le migrazioni.

Fasi chiave di una migrazione di dati di grandi dimensioni

Di solito è possibile suddividere una migrazione di grandi dimensioni nelle seguenti fasi:

- (Fase 1) Pianificazione della migrazione dei dati: in questa fase, stai cercando di capire perché stai migrando e con che tipo di dati stai lavorando. Le attività di pianificazione includono:
  - Capire perché vuoi migrare
  - Assemblare un team che vi aiuti in tutti gli aspetti della migrazione.
  - Identificazione delle posizioni, dei formati e dei modelli di utilizzo dei dati

    - Valutazione delle risorse hardware disponibili e dei requisiti di rete (in caso di migrazione da un data center locale)
    - Esegui test proof of concept (POC) DataSync per stimare le tempistiche di migrazione, pianificare le finestre temporali e avere un'idea di come devi configurare DataSync
- (Fase 2) Implementazione della migrazione di grandi dimensioni dei dati: a questo punto, stai convalidando il piano e avviando la migrazione. Le attività di implementazione includono:
    - Convalida del piano di migrazione
    - Esecuzione di passaggi graduali che includono il monitoraggio e la verifica dei trasferimenti di dati come previsto
    - Ottimizzazione e regolazione secondo necessità tra ogni taglio
    - Ripulire le risorse inutilizzate una volta terminato

Risorse aggiuntive

AWS Prescriptive Guidance dispone delle seguenti risorse che possono aiutarti a pianificare e implementare una migrazione su larga scala. Utilizza questa guida per capire come DataSync può funzionare nel contesto di processi e attività di migrazione comuni.

- Grandi migrazioni verso il cloud AWS
- Strategia e best practice per migrazioni di AWS grandi dimensioni
- Migra i file system condivisi in una migrazione di AWS grandi dimensioni: questa risorsa include una cartella di lavoro SFS-Discovery-Workbook che è possibile scaricare e utilizzare per pianificare una migrazione a livello di condivisione di file.

Fase 1: pianificazione della migrazione di dati di grandi dimensioni

La pianificazione è essenziale durante la migrazione di un set di dati di grandi dimensioni. Devi comprendere i dati che stai migrando, le motivazioni alla base della migrazione e come AWS DataSync puoi aiutarti a portare i dati dove vuoi.

Argomenti

- Raccolta dei requisiti per la migrazione
- Esecuzione di un DataSync proof of concept
- Stima delle tempistiche di migrazione

Raccolta dei requisiti per la migrazione

Il primo passaggio di una migrazione di dati di grandi dimensioni richiede la raccolta di una varietà di informazioni all'interno dell'organizzazione.

Queste informazioni consentono di creare un processo di migrazione, che per le migrazioni di grandi dimensioni può includere trasferimenti multipli e procedure per il trasferimento delle operazioni (eseguite a ondate) dallo storage di origine a quello di destinazione.

Comprendere il motivo per cui si desidera effettuare la migrazione

Prima di iniziare la migrazione a AWS, devi capire chiaramente perché stai migrando i tuoi dati. Questo aiuta ad affrontare le sfide comuni della migrazione, come il rispetto delle scadenze, la gestione delle risorse e il coordinamento tra i team.

Se hai bisogno di aiuto per determinare le tue motivazioni alla base della migrazione, rispondi a queste domande:

- Stai liberando spazio di archiviazione in locale?
- Stai rispettando le scadenze dei contratti di assistenza hardware?
- È per uscire da un data center?
- Qual è la tua tempistica di migrazione?
- Stai trasferendo dati da un altro spazio di archiviazione cloud?
- Stai migrando set di dati parziali o completi?
- È per l'archiviazione dei dati?
- Le applicazioni o gli utenti necessitano di un accesso regolare a questi dati?

Capire la logistica

Affrontate alcuni aspetti logistici di base relativi all'ambiente di storage, alla migrazione e alla vostra organizzazione:

1. Ottieni una conoscenza di base della tua attuale infrastruttura di storage dei dati.
2. Verifica se hai bisogno di un DataSync agente. Ad esempio, è necessario un agente se si esegue il trasferimento da uno storage locale.
3. Se hai bisogno di un agente, assicurati di aver compreso i requisiti dell'agente:

- Un agente può essere eseguito come macchina virtuale (VM) su VMware ESXi hypervisor KVM (Linux Kernel-based Virtual Machine) e Microsoft Hyper-V. Puoi anche implementare un agente come EC2 istanza Amazon all'interno AWS.
- Le migrazioni di grandi dimensioni richiedono in genere un uso intensivo della memoria. Assicurati che il tuo agente disponga di RAM sufficiente.

4. Identifica le principali parti interessate dei tuoi dipartimenti dirigenziali, di rete, di storage e IT che devono essere coinvolte nella migrazione. Sono inclusi:
   - Trova un leader unico che si dedichi al progetto e ai suoi risultati.
   - Determina chi è responsabile della proprietà e della classificazione dei dati da migrare.
   - Identifica chi gestisce la tua fonte e chi alla fine gestirà il servizio AWS di storage verso cui stai migrando.
   - Scopri chi creerà e gestirà qualsiasi altro processo per i tuoi dati una volta inseriti AWS.
5. Stabilisci canali di comunicazione tra i reparti.
6. Crea un piano di rollback per gli imprevisti.
7. Documenta l'intero processo di migrazione, comprese le procedure di ondata, convalida e cutover. Utilizzalo come manuale per l'intera migrazione. Aggiornerai questo processo man mano che pianifichi e implementerai la migrazione.

Revisione dei dati che stai migrando

Collabora con i team di storage e applicazione per analizzare le caratteristiche dei dati che stai migrando. Queste informazioni ti aiutano a determinare una strategia di migrazione che puoi utilizzare. DataSync

Indice

- Definizione dei modelli di utilizzo dei dati
- Identificazione della struttura e del layout dei dati
- Documentazione di condivisioni e cartelle
- Analisi delle dimensioni dei file

Definizione dei modelli di utilizzo dei dati

- Per i dati utilizzati attivamente con modifiche frequenti, pianifica più ondate di trasferimenti incrementali per evitare di interrompere le operazioni aziendali.
- Per i dati di sola lettura che potrebbero essere considerati archiviati, potrebbe non essere necessario pianificare ondate di dati.
- Se hai una combinazione di modelli di utilizzo dei dati, pianifica ondate che migrano questi diversi set di dati separatamente. Ad esempio, potresti avere un'ondata per i dati di archiviazione, mentre il resto delle ondate potrebbe essere dedicato alla migrazione dei dati attivi.

Identificazione della struttura e del layout dei dati

- Determina se i dati sono organizzati per periodi di tempo (anno, mese, giorno) o altri modelli.
- Usa questa struttura organizzativa per pianificare le tue ondate di migrazione. Ad esempio, potresti migrare un anno di dati di archivio durante un'unica ondata.

Documentazione di condivisioni e cartelle

- Crea un inventario di condivisioni e cartelle (incluso il numero di file o oggetti per ciascuna).
- Identifica condivisioni e cartelle con set di dati attivi. Questi potrebbero richiedere trasferimenti incrementali durante la migrazione.
- Rivedi le DataSync quote. Questo può aiutarti a pianificare come partizionare il set di dati durante la configurazione. DataSync

Analisi delle dimensioni dei file

- Aspettatevi una maggiore velocità di trasmissione dei dati per i trasferimenti con file più grandi (MB o GB) rispetto ai file più piccoli (KB).
- Se lavori con molti file più piccoli, aspettati un maggior numero di operazioni sui metadati sul tuo sistema di storage e una minore velocità di trasmissione dei dati. DataSyncesegue queste operazioni durante il confronto e la verifica delle posizioni di origine e di destinazione.

Identificazione dei requisiti di archiviazione

Per scegliere un servizio AWS di storage compatibile per la migrazione dei dati, è necessario valutare le caratteristiche e le prestazioni del sistema di storage di origine.

Queste informazioni possono inoltre aiutarvi a pianificare i trasferimenti per ridurre al minimo l'impatto sulle operazioni aziendali durante la migrazione.

Indice

- Determinazione del supporto per lo storage
- Revisione dei requisiti di conservazione dei metadati
- Raccolta di metriche prestazionali dallo storage di origine
- Scelta di un servizio AWS di archiviazione di destinazione

Determinazione del supporto per lo storage

DataSync può funzionare con una varietà di sistemi di storage che consentono l'accesso tramite client di storage di oggetti compatibili con NFS, SMB, HDFS e S3.

Se stai migrando da un altro spazio di archiviazione cloud, verifica che DataSync possa funzionare con quel provider. Per un elenco delle posizioni di origine supportate, vedi Con chi posso trasferire i miei dati AWS DataSync?

Revisione dei requisiti di conservazione dei metadati

DataSync può conservare i metadati del file o dell'oggetto durante un trasferimento. Il modo in cui i metadati vengono conservati dipende dalle località di trasferimento e dal fatto che tali sedi utilizzino tipi di metadati simili.

DataSync in alcuni casi necessita di autorizzazioni aggiuntive per conservare i metadati dei file, come gli elenchi di accesso discrezionali NTFS (). DACLs

Per ulteriori informazioni, consulta Comprendere come DataSync gestisce i metadati di file e oggetti.

Raccolta di metriche prestazionali dallo storage di origine

Misura gli IOPS di base e la velocità effettiva del disco durante i carichi di lavoro medi e di picco per lo storage di origine. Il trasferimento dei dati aggiunge un sovraccarico di I/O ai sistemi di storage di origine e di destinazione.

Confrontate questi dati sulle prestazioni con le specifiche del sistema di storage per determinare le risorse prestazionali disponibili.

Scelta di un servizio AWS di archiviazione di destinazione

A questo punto, potresti avere un'idea di quale servizio AWS di archiviazione abbia senso per i tuoi dati. In caso contrario, i modelli di utilizzo dei dati e le prestazioni di archiviazione sono un paio di aree a cui prestare attenzione quando si decide. Ad esempio, potresti prendere in considerazione Amazon S3 se disponi di dati di archivio e Amazon o FSx Amazon EFS per i dati attivi.

Per aiutarti a decidere lo storage basato su oggetti o file giusto per i tuoi dati, consulta Scelta di un AWS servizio di storage.

Definizione dei requisiti di rete

Per eseguire la migrazione dei dati DataSync, è necessario stabilire connessioni di rete tra lo storage di origine, l'agente e AWS. È inoltre necessario pianificare una larghezza di banda e un'infrastruttura di rete sufficienti.

Collabora con i tuoi tecnici di rete e gli amministratori di storage per definire i seguenti requisiti di rete.

Indice

- Valutazione della larghezza di banda di rete disponibile
- Stai valutando le opzioni per connettere la tua rete a AWS
- Scelta di un endpoint di servizio per la comunicazione con gli agenti
- Pianificazione di un'infrastruttura di rete sufficiente

Valutazione della larghezza di banda di rete disponibile

La larghezza di banda di rete disponibile influisce sulla velocità di trasferimento e sul tempo complessivo di migrazione. Se stai effettuando il trasferimento da un sistema di storage locale, procedi come segue:

- Collabora con il team di rete per determinare l'utilizzo medio e di picco della larghezza di banda.
- Identifica le finestre in cui puoi trasferire i dati ed evita di interrompere le operazioni quotidiane. Ciò informerà quando si verificheranno le ondate di migrazione e i trasferimenti.

Puoi controllare la quantità di larghezza di banda DataSync utilizzata. Per ulteriori informazioni, consulta Impostazione dei limiti di larghezza di banda per l'attività AWS DataSync.

Poiché i trasferimenti da altri sistemi di archiviazione cloud avvengono in genere sulla rete Internet pubblica, in genere tali trasferimenti comportano meno restrizioni e considerazioni sulla larghezza di banda.

Stai valutando le opzioni per connettere la tua rete a AWS

Considerate le seguenti opzioni per stabilire la connettività di rete per il DataSync trasferimento:

- AWS Direct Connect- Esamina gli esempi di architettura e routing per l'utilizzo di Direct Connect con DataSync. Puoi monitorare l'attività di Direct Connect utilizzando Amazon CloudWatch.
- VPN: AWS Site-to-Site VPNoffre una velocità di trasmissione fino a 1,25 Gbps per tunnel.
- Internet pubblico: contatta il tuo provider di servizi Internet per i dati sull'utilizzo della rete.

Scelta di un endpoint di servizio per la comunicazione con gli agenti

DataSync gli agenti utilizzano gli endpoint del servizio per comunicare con il DataSync servizio. Il tipo di endpoint utilizzato dipende dalla modalità di connessione alla rete. AWS

Pianificazione di un'infrastruttura di rete sufficiente

Per ogni attività di trasferimento creata, genera e gestisce DataSync automaticamente l'infrastruttura di rete per i trasferimenti di dati. Questa infrastruttura è nota come interfacce di rete o interfacce di rete elastiche, che sono componenti di rete logici in un cloud privato virtuale (VPC) di Amazon che rappresentano schede di rete virtuali. Per ulteriori informazioni, consulta la Amazon EC2 User Guide.

Ogni interfaccia di rete utilizza un singolo indirizzo IP nella sottorete VPC di destinazione. Per assicurarti di disporre di un'infrastruttura di rete sufficiente per la migrazione, procedi come segue:

- Annota il numero di interfacce di rete che DataSync verranno create per la posizione di DataSync destinazione.
- Accertatevi che la sottorete disponga di indirizzi IP sufficienti per le vostre DataSync attività. Ad esempio, un'attività che utilizza un agente richiede quattro indirizzi IP. Se crei quattro attività per la migrazione, significa che hai bisogno di 16 indirizzi IP disponibili nella sottorete.

Esecuzione di un DataSync proof of concept

L'esecuzione di un proof of concept (POC) AWS DataSync consente di convalidare i seguenti aspetti della pianificazione della migrazione dei dati:

- Verifica la connettività di rete tra le posizioni di origine e di destinazione.
- Convalida la configurazione iniziale dell' DataSync attività.
- Misura le prestazioni di trasferimento dei dati.
- Stima le tempistiche di migrazione.
- Definisci i criteri di successo con le principali parti interessate che lavorano alla migrazione.

Inizia con il tuo proof of concept

1. Crea il tuo DataSync agente:
    1. Implementa il tuo agente.
    2. Scegli un endpoint di servizio per il tuo agente.
    3. Attiva il tuo agente.
    4. Verifica le connessioni di rete del tuo agente.
2. Seleziona un piccolo sottoinsieme di dati che rappresenti i dati di cui stai migrando.

    Ad esempio, se l'archivio di origine contiene una combinazione di file grandi e piccoli, il sottoinsieme di dati che trasferisci nel POC dovrebbe rispecchiare tale situazione. In questo modo è possibile ottenere una comprensione preliminare delle prestazioni dei sistemi di storage, della rete e DataSync
3. Crea una posizione DataSync di origine per il tuo sistema di archiviazione cloud locale o di altro tipo.
4. Crea una posizione di DataSync destinazione per il tuo servizio AWS di archiviazione.
5. Crea un'attività di DataSync trasferimento con un filtro che trasferisce solo il sottoinsieme di dati.
6. Inizia la tua DataSync attività.
7. Raccogli le metriche relative alle prestazioni di trasferimento monitorando quanto segue:
    - Velocità effettiva dei dati e dei file relativi all'esecuzione delle attività. È possibile farlo tramite la DataSync console o l'DescribeTaskExecutionoperazione. Se utilizzi`DescribeTaskExecution`, ecco come calcoli queste metriche:
        - Velocità effettiva dei dati: Dividi per `BytesWritten` `TransferDuration`
        - Velocità effettiva dei file: Dividi per `FilesTransferred` `TransferDuration`
    - Utilizzo dello storage di origine e destinazione. Collaborate a stretto contatto con gli amministratori dello storage per ottenere queste informazioni.

- Utilizzo della rete.

8. Verifica i dati trasferiti nella posizione di destinazione:

   - Esamina i CloudWatch registri per individuare eventuali errori di esecuzione delle attività.
   - Verifica che le autorizzazioni e i metadati siano conservati nella posizione di destinazione.
   - Verifica che le applicazioni e gli utenti possano accedere ai dati di destinazione come previsto.
   - Risolvete eventuali problemi riscontrati. Per ulteriori informazioni, consulta Risoluzione dei AWS DataSync problemi.

9. Esegui l'attività ancora qualche volta per farti un'idea del tempo necessario DataSync per preparare, trasferire e verificare i dati. Per ulteriori informazioni, consulta Stati di esecuzione delle attività.

   Se esegui un'attività più di una volta, DataSync per impostazione predefinita esegue un trasferimento incrementale e copia solo i dati modificati dall'esecuzione precedente dell'attività.

   Sebbene il tempo di trasferimento sia probabilmente più breve per i trasferimenti incrementali, DataSync prepareremo sempre il trasferimento allo stesso modo, scansionando e confrontando le posizioni per identificare cosa trasferire. Puoi utilizzare questi tempi di preparazione per stimare le tempistiche limite per la migrazione.

10. Se necessario, aggiorna il piano di migrazione in base a ciò che hai appreso durante il POC.

Stima delle tempistiche di migrazione

Utilizzando le informazioni raccolte fino a questo punto, puoi stimare il tempo necessario per la migrazione. AWS DataSync

Stima delle tempistiche di trasferimento dei dati

È possibile stimare il tempo necessario DataSync per il trasferimento dei dati in base alle seguenti informazioni raccolte durante la raccolta dei requisiti di migrazione e al DataSync proof of concept (POC):

- La larghezza di banda di rete disponibile
- Metriche di utilizzo dello storage di origine e destinazione
- Metriche prestazionali ricavate dal tuo POC DataSync

Per stimare una tempistica di trasferimento dei dati

1. Confrontate la velocità di trasmissione di dati e file del POC con la larghezza di banda di rete disponibile.
2. Se la velocità effettiva è inferiore alla larghezza di banda disponibile (ad esempio 300 MiB/s per la velocità effettiva con 10 Gbps di larghezza di banda di rete), valuta la possibilità di partizionare il set di dati in più attività per massimizzare l'utilizzo della larghezza di banda.

   DataSync dispone di alcune opzioni per il partizionamento del set di dati. Per ulteriori informazioni, consulta Accelerazione della migrazione con il partizionamento dei dati.
3. Calcola quanti giorni impiega un trasferimento utilizzando la seguente formula, che fornisce un tempo minimo teorico di trasferimento:

   ```
   (DATA_SIZE * 8 bits per byte)/(CIRCUIT * NETWORK_UTILIZATION percentage * 3600
    seconds per hour * AVAILABLE_HOURS) = Number of days
   ```

   Quando usi questa formula, sostituisci quanto segue con i tuoi valori:

   - `DATA_SIZE`: La quantità di dati da migrare (espressa in byte).
   - `CIRCUIT`: la larghezza di banda di rete disponibile (espressa in bit al secondo).
   - `NETWORK_UTILIZATION`: La percentuale della rete utilizzata.
   - `AVAILABLE_HOURS`: Il numero di ore operative disponibili in ogni giorno.

   Ad esempio, si calcola una migrazione con 100 TB di dati, una connessione Internet da 1 Gbps, l'80% di utilizzo della rete e una disponibilità 24 ore al giorno nel modo seguente:

   ```
   (100,000,000,000,000 bytes * 8) / (1,000,000,000 bps * 0.80 * 3600 *
   24) = 11.57 days
   ```

   In questo caso, la migrazione richiederebbe quasi 12 giorni prima di tenere conto delle condizioni del mondo reale.
4. Modifica la durata del trasferimento calcolata per tenere conto delle condizioni del mondo reale:

   - Fluttuazioni delle prestazioni di rete
   - Variazioni delle prestazioni di archiviazione
   - Tempo di inattività tra le ondate di migrazione

Stima delle tempistiche limite

Se state migrando set di dati attivi, probabilmente avrete bisogno di modifiche per non interrompere le operazioni aziendali.

Non sottovalutate il tempo necessario per i cutover. Con migrazioni di grandi dimensioni, non è raro che le attività di cutover occupino fino al 30 percento del tempo complessivo di migrazione.

1. Valuta se è necessario eseguire operazioni di cutover a ondate per ridurre la quantità di dati analizzati alla ricerca di modifiche incrementali.

   Una strategia a tal fine consiste nel tagliare i set di dati partizionati in base a condivisioni, cartelle o sistemi di storage.
2. Verifica il tempo impiegato in genere DataSync per preparare, trasferire e verificare i dati durante il POC.

   Nota in particolare la durata di preparazione delle esecuzioni delle attività. Per trovare queste informazioni, esegui l'DescribeTaskExecutionoperazione, quindi controlla il valore di PrepareDurationper la durata (in millisecondi).
3. Stima quanto tempo potrebbe richiedere un cutover misurando il delta temporale tra le attività parallele.

   Per ulteriori informazioni sulle attività parallele, vedereAccelerazione della migrazione con il partizionamento dei dati.
4. Usa la stima del cutover per pianificare i cutover. Si tratta essenzialmente di finestre di manutenzione in cui i dati di origine non possono essere modificati.

Passaggi successivi

Dopo aver stimato le tempistiche, sei pronto per iniziare a implementare la migrazione.

Fase 2: implementazione della migrazione di grandi quantità di dati

Con le informazioni raccolte durante la pianificazione, è possibile iniziare a utilizzarle AWS DataSync per migrare al nuovo sistema di storage. Se non l'hai già fatto, ti consigliamo di consultare le risorse di AWS Prescriptive Guidance per migrazioni di grandi dimensioni.

Argomenti

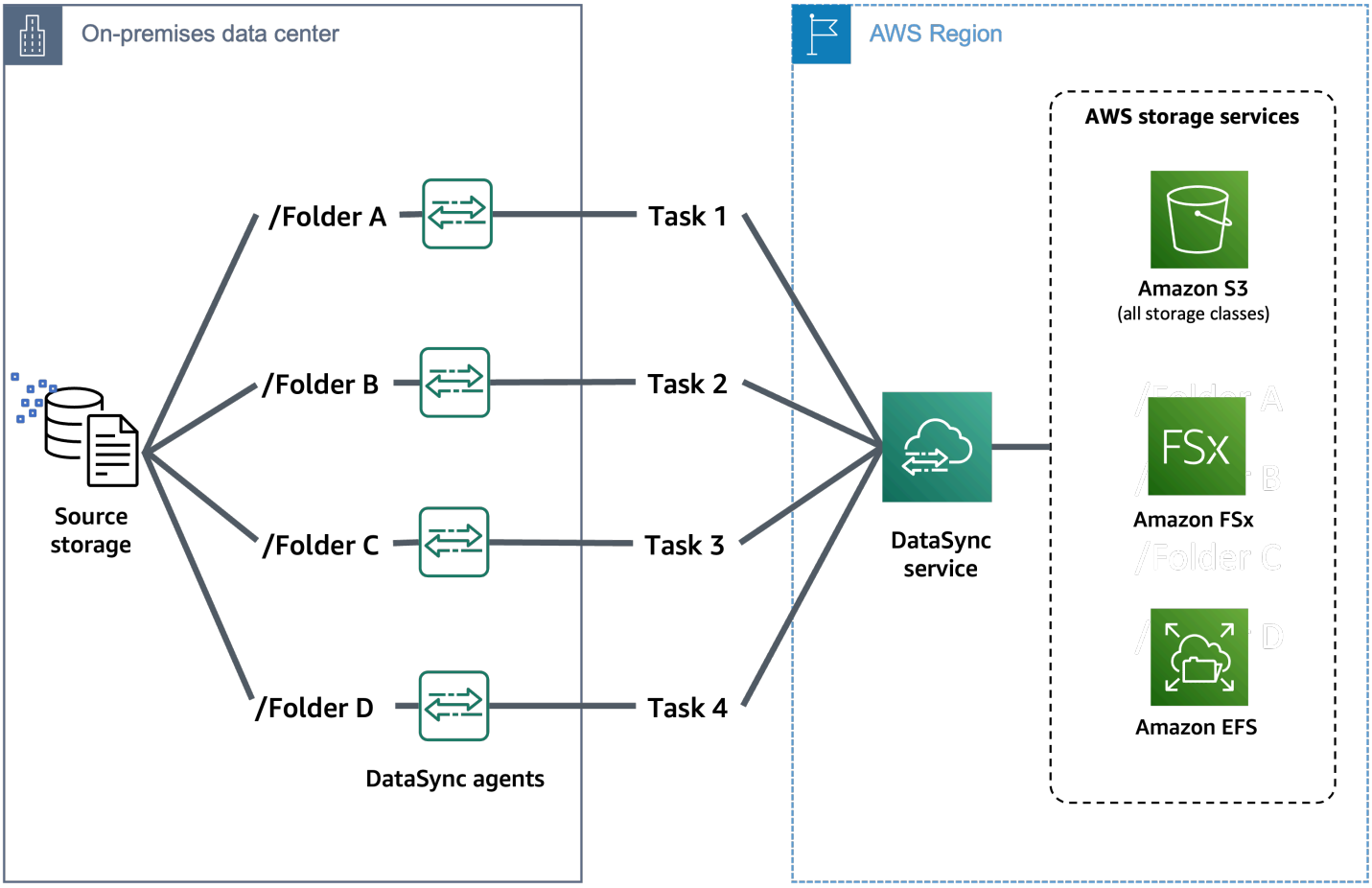
- Accelerazione della migrazione con il partizionamento dei dati
- Esecuzione delle attività DataSync di trasferimento
- Monitoraggio dei trasferimenti

Accelerazione della migrazione con il partizionamento dei dati

Con una migrazione di grandi dimensioni, consigliamo di partizionare il set di dati con più attività. DataSync Il partizionamento dei dati di origine tra più attività (e possibilmente tra agenti) consente di parallelizzare i trasferimenti e ridurre i tempi di migrazione.

Il partizionamento consente inoltre di rispettare le DataSync quote e semplifica il monitoraggio e il debug delle attività.

Il diagramma seguente mostra come è possibile utilizzare più DataSync attività e agenti per trasferire dati dalla stessa posizione di archiviazione di origine. In questo scenario, ogni attività si concentra su una cartella specifica nella posizione di origine. Per ulteriori informazioni ed esempi su questi approcci, vedi Come accelerare i trasferimenti di dati con architetture AWS DataSync scalabili orizzontalmente.



Partizionamento del set di dati per cartella o prefisso

Quando crei la posizione di DataSync origine, puoi specificare una cartella, una directory o un prefisso da cui leggere. DataSync Ad esempio, se stai migrando una condivisione di file con directory di primo livello, puoi creare più posizioni che specificano un percorso di directory diverso. Puoi quindi utilizzare queste posizioni per eseguire più DataSync attività durante la migrazione.

Partizionamento del set di dati con filtri

Puoi applicare filtri per includere o escludere dati dalla posizione di origine in un trasferimento. Nel contesto di una migrazione su larga scala, i filtri possono aiutarti ad assegnare le attività a porzioni specifiche del set di dati.

Ad esempio, se stai migrando dati di archivio organizzati per anno, puoi creare un filtro di inclusione da abbinare per uno o più anni specifici. Puoi anche modificare il filtro ogni volta che esegui l'attività in modo che corrisponda a un anno diverso.

Partizionamento del set di dati con manifesti

Un manifesto è un elenco di file o oggetti che si desidera trasferire. DataSync Con un manifesto, DataSync non è necessario leggere tutto in una posizione di origine per determinare cosa trasferire.

È possibile creare manifesti a partire dagli inventari dello storage di origine o tramite approcci basati sugli eventi (ad esempio, vedi Implementazione AWS DataSync con centinaia di milioni di oggetti). È inoltre possibile utilizzare un manifesto diverso ogni volta che si avvia un'attività, in modo da trasferire diversi set di dati con la stessa attività.

Esecuzione delle attività DataSync di trasferimento

Durante ciascuna delle vostre ondate di migrazione, il trasferimento dei dati di solito segue lo stesso processo generale:

1. Esegui un trasferimento iniziale completo dei tuoi dati.
2. Verifica i dati nella destinazione.
3. Esegui trasferimenti incrementali per tutti i dati che potrebbero essere cambiati rispetto al trasferimento iniziale.
4. Riduci le operazioni alla posizione di destinazione.
5. Rivedi i risultati di cutover.

Esecuzione delle attività

Probabilmente dovrai eseguire le attività di DataSync trasferimento durante l'orario lavorativo per ridurre al minimo il tempo complessivo di migrazione. In queste situazioni è normale eseguire un trasferimento completo iniziale seguito da trasferimenti incrementali che tengano conto delle modifiche alla posizione di origine da parte di utenti e applicazioni.

Per evitare problemi relativi alla rete durante l'orario lavorativo, puoi limitare la quantità di larghezza di banda utilizzata dalle tue attività. Per ulteriori informazioni, consulta Impostazione dei limiti di larghezza di banda per l'attività AWS DataSync.

1. Esegui un trasferimento completo iniziale:
    a. Avvia la tua DataSync attività (o le attività se esegui attività in parallelo).
    b. Monitora l'avanzamento e le prestazioni delle esecuzioni delle attività.

c. Verifica che i dati siano stati trasferiti nel modo previsto (ad esempio, i metadati dei file vengano conservati).

2. Esegui trasferimenti incrementali:

   a. Pianifica le tue attività in modo che vengano eseguite periodicamente.

   b. Monitora l'esecuzione delle attività e correggi gli errori, se riscontrati.

Esecuzione di un cutover

Dopo i trasferimenti iniziali e incrementali, è possibile avviare il processo di trasferimento delle operazioni verso la località di destinazione.

1. Avvia la finestra di manutenzione programmata.
2. Aggiorna il sistema di storage di origine in modo che sia di sola lettura per applicazioni e utenti.
3. Esegui i trasferimenti incrementali finali per copiare i delta rimanenti tra le posizioni di origine e di destinazione.
4. Esegui una convalida completa dei dati (ad esempio, esaminando i CloudWatch log e i report delle attività).
5. Sposta le applicazioni e gli utenti nel nuovo ambiente della località di destinazione.
6. Verifica la funzionalità dell'applicazione e assicurati che gli utenti possano accedere ai dati nella posizione di destinazione.
7. Pianifica una riunione retrospettiva per esaminare il trasferimento con i team di migrazione. Poni le seguenti domande di esempio:

   - Il cutover ha avuto successo? In caso contrario, qual era il problema?
   - Abbiamo utilizzato tutta la larghezza di banda disponibile?
   - Lo storage di origine e di destinazione è stato completamente utilizzato?
   - Possiamo ottenere una maggiore velocità di trasmissione dei dati con attività aggiuntive?
   - Dobbiamo pianificare una finestra di manutenzione più lunga?

8. Se necessario, aggiorna il piano di migrazione prima di iniziare la fase successiva.

Monitoraggio dei trasferimenti

AWS DataSync offre diverse opzioni di monitoraggio per aiutarti a convalidare ed eseguire il debug del trasferimento.

Monitoraggio dei trasferimenti tramite metriche CloudWatch

Puoi creare CloudWatch dashboard personalizzate con metriche relative all'esecuzione delle tue DataSync attività. Per ulteriori informazioni, consulta Monitoraggio dei trasferimenti di dati con i CloudWatch parametri di Amazon.

Monitoraggio dei trasferimenti con report sulle attività

Se trasferisci milioni di file o oggetti, prendi in considerazione l'utilizzo dei report sulle attività. I report sulle attività forniscono informazioni dettagliate su quali DataSync tentativi di trasferire, ignorare, verificare ed eliminare durante l'esecuzione di un'attività. Per ulteriori informazioni, consulta Monitoraggio dei trasferimenti di dati con report sulle attività.

Puoi anche visualizzare i report delle attività utilizzando AWS servizi come AWS Glue Amazon Athena e Amazon. QuickSight Per ulteriori informazioni, consulta lo AWS Storage Blog.

Monitoraggio dei trasferimenti con CloudWatch Logs

Come minimo, ti consigliamo di configurare l'attività per registrare le informazioni di base e gli errori di trasferimento. Per ulteriori informazioni, consulta Monitoraggio dei trasferimenti di dati con Amazon CloudWatch Logs.

AWS DataSync API

Oltre a AWS Management Console and AWS CLI, puoi utilizzare l' AWS DataSync API per configurare e gestire DataSync con AWS SDKs.

Argomenti

- Azioni
- Tipi di dati
- Errori comuni
- Parametri comuni

Azioni

Sono supportate le operazioni seguenti:

- 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

Interrompe l'esecuzione di un' AWS DataSync attività in corso. Il trasferimento di alcuni file viene interrotto bruscamente. I contenuti dei file trasferiti nella destinazione potrebbero essere incompleti o non coerenti con i file di origine.

Tuttavia, se iniziate l'esecuzione di una nuova attività utilizzando la stessa operazione e ne consentite il completamento, il contenuto del file nella destinazione sarà completo e coerente. Questo vale per altri errori imprevisti che interrompono l'esecuzione di un'attività. In tutti questi casi, il trasferimento viene completato DataSync correttamente all'avvio dell'esecuzione successiva dell'attività.

Sintassi della richiesta

```
{
   "TaskExecutionArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

TaskExecutionArn

L'Amazon Resource Name (ARN) dell'esecuzione dell'attività da interrompere.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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}$`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateAgent

Attiva un AWS DataSync agente da distribuire nel tuo ambiente di storage. Il processo di attivazione associa l'agente al tuo. Account AWS

Se non hai ancora implementato un agente, vedi Ho bisogno di un DataSync agente?

Sintassi della richiesta

```
{
   "ActivationKey": "string",
   "AgentName": "string",
   "SecurityGroupArns": [ "string" ],
   "SubnetArns": [ "string" ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "VpcEndpointId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ActivationKey

Specifica la chiave di attivazione del tuo DataSync agente. Se non disponi di una chiave di attivazione, vedi Attivazione del tuo agente.

Tipo: stringa

Limiti di lunghezza: lunghezza massima di 29.

Modello: `[A-Z0-9]{5}(-[A-Z0-9]{5}){4}`

Campo obbligatorio: sì

AgentName

Specificate un nome per il vostro agente. Ti consigliamo di specificare un nome facile da ricordare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

SecurityGroupArns

Speciifica l'Amazon Resource Name (ARN) del gruppo di sicurezza che consente il traffico tra l'agente e l'endpoint del servizio VPC. È possibile specificare un solo ARN.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Campo obbligatorio: no

SubnetArns

Speciifica l'ARN della sottorete in cui si trova l'endpoint del servizio VPC. È possibile specificare un solo ARN.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/.*$`

Campo obbligatorio: no

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse. AWS Ti consigliamo di creare almeno un tag per il tuo agente.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

VpcEndpointId

Specifica l'ID dell'endpoint del servizio VPC che stai utilizzando. Ad esempio, ha il seguente aspetto: un ID endpoint VPC. `vpce-01234d5aff67890e1`

> **Important**
>
> L'endpoint del servizio VPC utilizzato deve includere il nome del DataSync servizio (ad esempio,). `com.amazonaws.us-east-2.datasync`

Tipo: stringa

Modello: `^vpce-[0-9a-f]{17}$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "AgentArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AgentArn

L'ARN dell'agente che hai appena attivato. Utilizzate l'ListAgentsoperazione per restituire un elenco di agenti nel vostro Account AWS and Regione AWS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

L'esempio seguente attiva un agente. DataSync

```
{
    "ActivationKey": "AAAAA-1AAAA-BB1CC-33333-EEEEE",
    "AgentName": "MyAgent",
    "Tags": [{
        "Key": "Job",
        "Value": "TransferJob-1"
    }]
}
```

Risposta di esempio

La risposta restituisce l'ARN dell'agente attivato.

```
{
    "AgentArn": "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44baca3"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationAzureBlob

Crea una posizione di trasferimento per un contenitore Microsoft Azure Blob Storage. AWS DataSync può usare questa posizione come origine o destinazione di trasferimento. Puoi effettuare trasferimenti con o senza un DataSync agente che si connetta al tuo contenitore.

Prima di iniziare, assicurati di sapere come DataSync accede all'archiviazione BLOB di Azure e come funziona con i livelli di accesso e i tipi di blob.

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessTier

Speciifica il livello di accesso in cui desideri trasferire gli oggetti o i file. Ciò si applica solo quando si utilizza la posizione come destinazione di trasferimento. Per ulteriori informazioni, consulta Livelli di accesso.

Tipo: stringa

Valori validi: `HOT | COOL | ARCHIVE`

Campo obbligatorio: no

AgentArns

(Facoltativo) Specifica l'Amazon Resource Name (ARN) dell'agente che può connettersi DataSync al tuo contenitore Azure Blob Storage. Se stai configurando un trasferimento tra cloud senza agenti, non è necessario specificare un valore per questo parametro.

È possibile specificare più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti per il trasferimento.

> **Note**
>
> Assicurati di configurare correttamente questo parametro quando crei per la prima volta la tua posizione di archiviazione. Non è possibile aggiungere o rimuovere agenti da una posizione di archiviazione dopo averla creata.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

AuthenticationType

Specifica il metodo di autenticazione DataSync usato per accedere al tuo archivio BLOB di Azure. DataSync può accedere all'archiviazione BLOB utilizzando una firma ad accesso condiviso (SAS).

Tipo: stringa

Valori validi: `SAS | NONE`

Campo obbligatorio: sì

BlobType

Speciifica il tipo di blob che vuoi che siano i tuoi oggetti o file quando li trasferisci in Azure Blob Storage. Attualmente, supporta DataSync solo lo spostamento di dati in Azure Blob Storage come block blob. Per altre informazioni sui tipi di blob, consulta la documentazione di Azure Blob Storage.

Tipo: stringa

Valori validi: `BLOCK`

Campo obbligatorio: no

CmkSecretConfig

Specifica le informazioni di configurazione per un segreto DataSync gestito, che include il token di autenticazione DataSync utilizzato per accedere a una posizione di AzureBlob archiviazione specifica, con un codice gestito dal cliente. AWS KMS key

Quando includi questo parametro come parte di una `CreateLocationAzureBlob` richiesta, fornisci solo l'ARN della chiave KMS. DataSync utilizza questa chiave KMS insieme al token di autenticazione specificato per creare un segreto DataSync gestito per `SasConfiguration` memorizzare le credenziali di accesso alla posizione.

Assicurati che DataSync abbia il permesso di accedere alla chiave KMS specificata.

> **Note**
>
> Puoi utilizzare `CmkSecretConfig` (con`SasConfiguration`) o `CustomSecretConfig` (senza`SasConfiguration`) per fornire le credenziali per una `CreateLocationAzureBlob` richiesta. Non fornire entrambi i parametri per la stessa richiesta.

Tipo: oggetto CmkSecretConfig

Campo obbligatorio: no

ContainerUrl

Speciifica l'URL del contenitore Azure Blob Storage coinvolto nel trasferimento.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 325.

Modello: `^https:\/\/[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}\/[a-z0-9](-?[a-z0-9]){2,62}$`

Campo obbligatorio: sì

CustomSecretConfig

Specifica le informazioni di configurazione per un segreto di Secrets Manager gestito dal cliente in cui il token di autenticazione per una posizione di AzureBlob archiviazione è archiviato in testo semplice. Questa configurazione include l'ARN segreto e l'ARN per un ruolo IAM che fornisce l'accesso al segreto.

> **Note**
>
> È possibile utilizzare `CmkSecretConfig` (con`SasConfiguration`) o `CustomSecretConfig` (senza`SasConfiguration`) per fornire le credenziali per una richiesta. `CreateLocationAzureBlob` Non fornire entrambi i parametri per la stessa richiesta.

Tipo: oggetto CustomSecretConfig

Campo obbligatorio: no

SasConfiguration

Speciifica la configurazione SAS che consente di accedere DataSync al tuo Azure Blob Storage.

> **Note**
>
> Se fornisci un token di autenticazione utilizzando`SasConfiguration`, ma non fornisci dettagli di configurazione segreti utilizzando `CmkSecretConfig`

oCustomSecretConfig, DataSync archivia il token utilizzando il segreto del gestore dei segreti del tuo AWS account.

Tipo: oggetto AzureBlobSasConfiguration

Campo obbligatorio: no

Subdirectory

Specificate i segmenti di percorso se desiderate limitare il trasferimento a una directory virtuale del contenitore (ad esempio,/my/images).

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 1024.

Modello: ^[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}\p{C}]*$

Campo obbligatorio: no

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse AWS . Ti consigliamo di creare almeno un tag con il nome per la località di trasferimento.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'ARN della posizione di trasferimento di Azure Blob Storage che hai creato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationEfs

Crea una posizione di trasferimento per un file system Amazon EFS. AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Prima di iniziare, assicurati di aver compreso come DataSync accede ai file system Amazon EFS.

Sintassi della richiesta

```
{
   "AccessPointArn": "string",
   "Ec2Config": {
      "SecurityGroupArns": [ "string" ],
      "SubnetArn": "string"
   },
   "EfsFilesystemArn": "string",
   "FileSystemAccessRoleArn": "string",
   "InTransitEncryption": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessPointArn

Speciifica l'Amazon Resource Name (ARN) del punto di accesso utilizzato per DataSync montare il file system Amazon EFS.

Per ulteriori informazioni, consulta Accesso ai file system con restrizioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

Campo obbligatorio: no

Ec2Config

Speciifica la sottorete e i gruppi di sicurezza DataSync utilizzati per connettersi a uno degli obiettivi di montaggio del file system Amazon EFS.

Tipo: oggetto Ec2Config

Campo obbligatorio: sì

EfsFilesystemArn

Speciifica l'ARN per il tuo file system Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Campo obbligatorio: sì

FileSystemAccessRoleArn

Specifica un ruolo AWS Identity and Access Management (IAM) che consente di accedere DataSync al file system Amazon EFS.

Per informazioni sulla creazione di questo ruolo, consulta Creazione di un ruolo DataSync IAM per l'accesso al file system.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Campo obbligatorio: no

InTransitEncryption

Specifica se desideri DataSync utilizzare la crittografia Transport Layer Security (TLS) 1.2 quando trasferisce dati da o verso il tuo file system Amazon EFS.

Se specifichi un punto di accesso utilizzando `AccessPointArn` o un ruolo IAM utilizzando `FileSystemAccessRoleArn`, è necessario impostare questo parametro su `TLS1_2`.

Tipo: stringa

Valori validi: `NONE | TLS1_2`

Campo obbligatorio: no

Subdirectory

Specifica un percorso di montaggio per il tuo file system Amazon EFS. È qui che DataSync legge o scrive i dati sul tuo file system (a seconda che si tratti di una posizione di origine o di destinazione).

Per impostazione predefinita, DataSync utilizza la directory principale (o il punto di accesso, se fornito utilizzando`AccessPointArn`). È inoltre possibile includere sottodirectory utilizzando barre (ad esempio,). `/path/to/folder`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: no

Tags

Specifica la coppia chiave-valore che rappresenta un tag che si desidera aggiungere alla risorsa. Il valore può essere una stringa vuota. Questo valore consente di gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'Amazon Resource Name (ARN) della posizione del file system Amazon EFS che crei.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

L'esempio seguente crea una posizione per un file system Amazon EFS.

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

Richiesta di esempio: creazione di una posizione per un file system Amazon EFS con restrizioni

L'esempio seguente crea una posizione per un file system Amazon EFS con accesso limitato. In questo tipo di scenario, potrebbe essere necessario specificare i valori per `AccessPointArn` e `InTransitEncryption` nella richiesta. `FileSystemAccessRoleArn`

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

Risposta di esempio

Una risposta restituisce l'ARN della posizione del file system Amazon EFS.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-12abcdef012345678"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationFsxLustre

Crea una posizione di trasferimento per un file system Amazon FSx for Lustre. AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Prima di iniziare, assicurati di aver compreso come DataSync accedere ai file system FSx Lustre.

Sintassi della richiesta

```
{
   "FsxFilesystemArn": "string",
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

FsxFilesystemArn

Speciifica l'Amazon Resource Name (ARN) FSx del file system for Lustre.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Campo obbligatorio: sì

SecurityGroupArns

Speciifica i nomi delle risorse Amazon (ARNs) di un massimo di cinque gruppi di sicurezza che forniscono l'accesso al file system FSx for Lustre.

I gruppi di sicurezza devono essere in grado di accedere alle porte del file system. Il file system deve consentire anche l'accesso dai gruppi di sicurezza. Per informazioni sull'accesso al file system, consulta la Amazon FSx for Lustre User Guide.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Campo obbligatorio: sì

Subdirectory

Speciifica un percorso di montaggio per il file system FSx for Lustre. Il percorso può includere sottodirectory.

Quando la posizione viene utilizzata come fonte, DataSync legge i dati dal percorso di montaggio. Quando la posizione viene utilizzata come destinazione, DataSync scrive i dati nel percorso di montaggio. Se non includete questo parametro, DataSync utilizza la directory principale del file system (`/`).

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse AWS . È consigliabile creare almeno un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'Amazon Resource Name (ARN) della posizione del file system FSx for Lustre che hai creato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationFsxOntap

Crea una posizione di trasferimento per un file system Amazon FSx for NetApp ONTAP. AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Prima di iniziare, assicurati di aver compreso come DataSync accedere ai file system FSx ONTAP.

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Protocol

Speciifica il protocollo di trasferimento dati AWS DataSync utilizzato per accedere al tuo FSx file system Amazon.

Tipo: oggetto FsxProtocol

Campo obbligatorio: sì

SecurityGroupArns

Speciifica i gruppi EC2 di sicurezza Amazon che forniscono l'accesso alla sottorete preferita del tuo file system.

I gruppi di sicurezza devono consentire il traffico in uscita sulle seguenti porte (a seconda del protocollo utilizzato):

- NFS (Network File System): porte TCP 111, 635 e 2049
- SMB (Server Message Block): porta TCP 445

I gruppi di sicurezza del file system devono inoltre consentire il traffico in entrata sulle stesse porte.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Campo obbligatorio: sì

StorageVirtualMachineArn

Specifica l'ARN della macchina virtuale di archiviazione (SVM) nel file system in cui o da cui copiare i dati.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 162.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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,}$`

Campo obbligatorio: sì

Subdirectory

Specificate il percorso della condivisione di file nella SVM da cui desiderate trasferire i dati o da cui desiderate trasferire i dati.

Puoi specificare un percorso di giunzione (detto anche punto di montaggio), un percorso qtree (per condivisioni di file NFS) o un nome condivisione (per condivisioni di file SMB). Ad esempio, il percorso di montaggio potrebbe essere `/vol1`, `/vol1/tree1`, o `/share1`.

> **Note**
>
> Non specificare un percorso di giunzione nel volume radice dell'SVM. Per ulteriori informazioni, consulta Managing FSx for ONTAP Storage Virtual Machines nella Amazon FSx for NetApp ONTAP User Guide.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Campo obbligatorio: no

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse AWS . È consigliabile creare almeno un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

Specificate l'ARN della posizione FSx del file system for ONTAP che create.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationFsxOpenZfs

Crea una posizione di trasferimento per un file system Amazon FSx for OpenZFS. AWS DataSync può utilizzare questa posizione come fonte o destinazione per il trasferimento di dati.

Prima di iniziare, assicurati di aver compreso come DataSync accedere ai file system FSx OpenZFS.

> **Note**
>
> I parametri di richiesta relativi a SMB non sono supportati dall'operazione. `CreateLocationFsxOpenZfs`

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

FsxFilesystemArn

L'Amazon Resource Name (ARN) del file system FSx per OpenZFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Campo obbligatorio: sì

Protocol

Il tipo di protocollo AWS DataSync utilizzato per accedere al file system.

Tipo: oggetto FsxProtocol

Campo obbligatorio: sì

SecurityGroupArns

I gruppi ARNs di sicurezza utilizzati per configurare il file system FSx per OpenZFS.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Campo obbligatorio: sì

Subdirectory

Una sottodirectory nel percorso della posizione che deve iniziare con. `/fsx` DataSync utilizza questa sottodirectory per leggere o scrivere dati (a seconda che il file system sia una posizione di origine o di destinazione).

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[^\u0000\u0085\u2028\u2029\r\n]{1,4096}$`

Campo obbligatorio: no

Tags

La coppia chiave-valore che rappresenta un tag che si desidera aggiungere alla risorsa. Il valore può essere una stringa vuota. Questo valore consente di gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'ARN della posizione del FSx file system OpenZFS che hai creato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationFsxWindows

Crea una posizione di trasferimento per un file system Amazon FSx for Windows File Server. AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Prima di iniziare, assicuratevi di conoscere DataSync le modalità di accesso ai file system FSx di Windows File Server.

Sintassi della richiesta

```
{
   "Domain": "string",
   "FsxFilesystemArn": "string",
   "Password": "string",
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "User": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Domain

Speciifica il nome del dominio Windows a cui appartiene il file system FSx for Windows File Server.

Se nell'ambiente sono presenti più domini Active Directory, la configurazione di questo parametro assicura la DataSync connessione al file system corretto.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Campo obbligatorio: no

FsxFilesystemArn

Speciifica l'Amazon Resource Name (ARN) per FSx il file system per Windows File Server.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Campo obbligatorio: sì

Password

Speciifica la password dell'utente con le autorizzazioni per montare e accedere a file, cartelle e metadati dei file nel file system FSx per Windows File Server.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^.{0,104}$`

Campo obbligatorio: sì

SecurityGroupArns

Speciifica i gruppi ARNs di EC2 sicurezza Amazon che forniscono l'accesso alla sottorete preferita del tuo file system.

I gruppi di sicurezza specificati devono essere in grado di comunicare con i gruppi di sicurezza del tuo file system. Per informazioni sulla configurazione dei gruppi di sicurezza per l'accesso al file system, consulta la Amazon FSx for Windows File Server User Guide.

> **Note**
>
> Se scegli un gruppo di sicurezza che non consente connessioni dall'interno, esegui una delle seguenti operazioni:
>
> - Configura il gruppo di sicurezza per consentirgli di comunicare al suo interno.

- Scegli un gruppo di sicurezza diverso in grado di comunicare con il gruppo di sicurezza del target di montaggio.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Campo obbligatorio: sì

Subdirectory

Specifica un percorso di montaggio per il tuo file system utilizzando le barre. Qui è dove DataSync legge o scrive i dati (a seconda che si tratti di una posizione di origine o di destinazione).

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse AWS . È consigliabile creare almeno un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

User

Speciifica l'utente con le autorizzazioni per montare e accedere a file, cartelle e metadati dei file nel file system FSx per Windows File Server.

Per informazioni sulla scelta di un utente con il giusto livello di accesso per il trasferimento, consulta le autorizzazioni richieste FSx per le posizioni dei file server di Windows.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'ARN della posizione del file system FSx per Windows File Server che hai creato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationHdfs

Crea una posizione di trasferimento per un Hadoop Distributed File System (HDFS). AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Prima di iniziare, assicurati di aver compreso come DataSync accede ai cluster HDFS.

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArns

Gli Amazon Resource Names (ARNs) degli DataSync agenti che possono connettersi al tuo cluster HDFS.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: sì

AuthenticationType

Il tipo di autenticazione utilizzato per determinare l'identità dell'utente.

Tipo: stringa

Valori validi: `SIMPLE | KERBEROS`

Campo obbligatorio: sì

BlockSize

La dimensione dei blocchi di dati da scrivere nel cluster HDFS. La dimensione del blocco deve essere un multiplo di 512 byte. La dimensione predefinita del blocco è 128 mebibyte (MiB).

Tipo: integer

Intervallo valido: valore minimo di 1048576. Valore massimo di 1073741824.

Campo obbligatorio: no

KerberosKeytab

La tabella delle chiavi Kerberos (keytab) che contiene le mappature tra il principali Kerberos definiti e le chiavi crittografate. È possibile caricare il keytab da un file fornendo l'indirizzo del file.

> **Note**
>
> Questo parametro è obbligatorio se `KERBEROS` viene specificato per `AuthenticationType`.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 65536.

Campo obbligatorio: no

KerberosKrb5Conf

Il file `krb5.conf` che contiene le informazioni di configurazione di Kerberos. È possibile caricare il `krb5.conf` file fornendo l'indirizzo del file. Se stai usando AWS CLI, esegue la codifica base64 per te. Altrimenti, fornisci il testo con codifica base64.

> **Note**
>
> Questo parametro è obbligatorio se `KERBEROS` viene specificato per `AuthenticationType`.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 131072.

Campo obbligatorio: no

KerberosPrincipal

Il principale Kerberos con accesso ai file e alle cartelle sul cluster HDFS.

> **Note**
>
> Questo parametro è obbligatorio se `KERBEROS` viene specificato per `AuthenticationType`.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^.+$`

Campo obbligatorio: no

KmsKeyProviderUri

L'URI del Key Management Server (KMS) del cluster HDFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `^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$`

Campo obbligatorio: no

NameNodes

Il NameNode che gestisce lo spazio dei nomi HDFS. NameNode Esegue operazioni come l'apertura, la chiusura e la ridenominazione di file e directory. NameNode Contiene le informazioni per mappare blocchi di dati su. DataNodes È possibile utilizzarne solo uno NameNode.

Tipo: matrice di oggetti HdfsNameNode

Membri dell'array: numero minimo di 1 elemento.

Campo obbligatorio: sì

QopConfiguration

La configurazione QOP (Quality of Protection) specifica le impostazioni di protezione per le chiamate di procedura remota (RPC, Remote Procedure Call) e per il trasferimento dati configurate nel cluster del file system distribuito Hadoop (HDFS). Se non si specifica `QopConfiguration`, il valore predefinito di `RpcProtection` e `DataTransferProtection` sarà `PRIVACY`. Se si imposta `RpcProtection` o `DataTransferProtection`, l'altro parametro assume lo stesso valore.

Tipo: oggetto QopConfiguration

Campo obbligatorio: no

ReplicationFactor

Il numero DataNodes su cui replicare i dati durante la scrittura sul cluster HDFS. Per impostazione predefinita, i dati vengono replicati fino a tre. DataNodes

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 512.

Campo obbligatorio: no

SimpleUser

Il nome utente utilizzato per identificare il client sul sistema operativo host.

> **Note**
>
> Questo parametro è obbligatorio se `SIMPLE` viene specificato per `AuthenticationType`.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

Campo obbligatorio: no

Subdirectory

Una sottodirectory nel cluster HDFS. Questa sottodirectory viene utilizzata per leggere i dati da o scrivere i dati sul cluster HDFS. Se la sottodirectory non viene specificata, il valore predefinito sarà impostato su `/`.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

Tags

La coppia chiave-valore che rappresenta il tag che si desidera aggiungere alla posizione. Il valore può essere una stringa vuota. Si consiglia di utilizzare tag per assegnare un nome alle risorse.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'ARN della posizione del cluster HDFS di origine che crei.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationNfs

Crea una posizione di trasferimento per un file server Network File System (NFS). AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Prima di iniziare, assicuratevi di aver compreso come DataSync accede ai file server NFS.

Sintassi della richiesta

```
{
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
   },
   "ServerHostname": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MountOptions

Speciifica le opzioni che è DataSync possibile utilizzare per montare il file server NFS.

Tipo: oggetto NfsMountOptions

Campo obbligatorio: no

OnPremConfig

Speciifica l'Amazon Resource Name (ARN) DataSync dell'agente che può connettersi al tuo file server NFS.

Puoi specificare più di un agente. Per ulteriori informazioni, vedere Utilizzo di più DataSync agenti.

Tipo: oggetto OnPremConfig

Campo obbligatorio: sì

ServerHostname

Speciifica il nome DNS o l'indirizzo IP (IPv4 o IPv6) del file server NFS a cui si connette l' DataSync agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Campo obbligatorio: sì

Subdirectory

Specificate il percorso di esportazione nel file server NFS che desiderate montare. DataSync

Questo percorso (o una sottodirectory del percorso) è il luogo in cui vengono DataSync trasferiti i dati da o verso. Per informazioni sulla configurazione di un'esportazione per DataSync, consultate Accesso ai file server NFS.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]+$`

Campo obbligatorio: sì

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse. AWS È consigliabile creare almeno un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'ARN della posizione di trasferimento che hai creato per il tuo file server NFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente crea una posizione di DataSync trasferimento per un file server NFS.

Richiesta di esempio

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

Esempio

La risposta restituisce l'ARN della posizione NFS.

Risposta di esempio

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationObjectStorage

Crea una posizione di trasferimento per un sistema di storage di oggetti. AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati. È possibile effettuare trasferimenti con o senza un DataSyncagente.

Prima di iniziare, assicurati di aver compreso i prerequisiti per lavorare con i sistemi di storage DataSync a oggetti.

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessKey

Specifica la chiave di accesso (ad esempio, un nome utente) se sono necessarie credenziali per l'autenticazione con il server di storage di oggetti.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `^.*$`

Campo obbligatorio: no

AgentArns

(Facoltativo) Speciifica gli Amazon Resource Names (ARNs) degli DataSync agenti che possono connettersi al tuo sistema di storage di oggetti. Se stai configurando un trasferimento tra cloud senza agenti, non è necessario specificare un valore per questo parametro.

> **Note**
>
> Assicurati di configurare correttamente questo parametro quando crei per la prima volta la tua posizione di archiviazione. Non è possibile aggiungere o rimuovere agenti da una posizione di archiviazione dopo averla creata.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

BucketName

Specifica il nome del bucket di storage di oggetti coinvolto nel trasferimento.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 63 caratteri.

Modello: `^[a-zA-Z0-9_\-\+\.\(\)\$\p{Zs}]+$`

Campo obbligatorio: sì

CmkSecretConfig

Specifica le informazioni di configurazione per un segreto DataSync gestito, che include il `SecretKey` segreto DataSync utilizzato per accedere a una posizione di archiviazione degli oggetti specifica, con un segreto gestito dal cliente. AWS KMS key

Quando includi questo parametro come parte di una `CreateLocationObjectStorage` richiesta, fornisci solo l'ARN della chiave KMS. DataSync utilizza questa chiave KMS insieme al valore specificato per il `SecretKey` parametro per creare un DataSync -managed secret per memorizzare le credenziali di accesso alla posizione.

Assicurati che DataSync abbia il permesso di accedere alla chiave KMS specificata.

> **Note**
>
> Puoi utilizzare `CmkSecretConfig` (con`SecretKey`) o `CustomSecretConfig` (senza`SecretKey`) per fornire le credenziali per una `CreateLocationObjectStorage` richiesta. Non fornire entrambi i parametri per la stessa richiesta.

Tipo: oggetto CmkSecretConfig

Campo obbligatorio: no

CustomSecretConfig

Specifica le informazioni di configurazione per un segreto di Secrets Manager gestito dal cliente in cui la chiave segreta per una posizione di archiviazione degli oggetti specifica è archiviata in testo semplice. Questa configurazione include l'ARN segreto e l'ARN per un ruolo IAM che fornisce l'accesso al segreto.

> **Note**
>
> È possibile utilizzare `CmkSecretConfig` (con`SecretKey`) o `CustomSecretConfig` (senza`SecretKey`) per fornire le credenziali per una richiesta.

`CreateLocationObjectStorage` Non fornire entrambi i parametri per la stessa richiesta.

Tipo: oggetto CustomSecretConfig

Campo obbligatorio: no

SecretKey

Specifica la chiave segreta (ad esempio, una password) se sono necessarie credenziali per l'autenticazione con il server di storage di oggetti.

> **Note**
>
> Se fornisci un segreto utilizzando`SecretKey`, ma non fornisci dettagli di configurazione segreti utilizzando `CmkSecretConfig` o`CustomSecretConfig`, DataSync archivia il token utilizzando il segreto di Secrets Manager del tuo AWS account.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `^.*$`

Campo obbligatorio: no

ServerCertificate

Speciifica una catena di certificati DataSync per l'autenticazione con il sistema di archiviazione degli oggetti se il sistema utilizza un'autorità di certificazione (CA) privata o autofirmata. È necessario specificare un singolo `.pem` file con una catena di certificati completa (ad esempio,). `file:///home/user/.ssh/object_storage_certificates.pem`

La catena di certificati potrebbe includere:

- Il certificato del sistema di archiviazione degli oggetti
- Tutti i certificati intermedi (se presenti)
- Il certificato principale della CA firmataria

È possibile concatenare i certificati in un `.pem` file (che può contenere fino a 32768 byte prima della codifica in base64). Il `cat` comando di esempio seguente crea un file che include tre certificati: `object_storage_certificates.pem`

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

Per utilizzare questo parametro, `ServerProtocol` configurare su`HTTPS`.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 32768.

Campo obbligatorio: no

ServerHostname

Speciifica il nome di dominio o l'indirizzo IP (IPv4 o IPv6) del server di archiviazione degli oggetti a cui si connette DataSync l'agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Campo obbligatorio: sì

ServerPort

Specifica la porta su cui il server di storage di oggetti accetta il traffico di rete in ingresso (ad esempio la porta 443).

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 65536.

Campo obbligatorio: no

ServerProtocol

Specifica il protocollo utilizzato dal server di storage di oggetti per comunicare. Se non specificato, il valore predefinito è `HTTPS`.

Tipo: stringa

Valori validi: `HTTPS | HTTP`

Campo obbligatorio: no

Subdirectory

Specifica il prefisso dell'oggetto per il server di storage di oggetti. Se si tratta di una posizione di origine, copia DataSync solo gli oggetti con questo prefisso. Se si tratta di una posizione di destinazione, DataSync scrive tutti gli oggetti con questo prefisso.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: no

Tags

Specifica la coppia chiave-valore che rappresenta un tag che si desidera aggiungere alla risorsa. I tag ti aiutano a gestire, filtrare e cercare le risorse. È consigliabile creare un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

Speciifica l'ARN della posizione del sistema di storage degli oggetti che si crea.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationS3

Crea una posizione di trasferimento per un bucket Amazon S3. AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

> **Important**
>
> Prima di iniziare, assicurati di leggere i seguenti argomenti:
>
> - Considerazioni sulla classe di storage con le sedi Amazon S3
> - Valutazione dei costi delle richieste S3 durante l'utilizzo DataSync

Per ulteriori informazioni, consulta Configurazione dei trasferimenti con Amazon S3.

Sintassi della richiesta

```
{
   "AgentArns": [ "string" ],
   "S3BucketArn": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
   "S3StorageClass": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArns

(Amazon S3 solo su Outposts) Specifica l'Amazon Resource Name (ARN) dell'agente sul tuo Outpost. DataSync

Per ulteriori informazioni, consulta Deploy your agent on. DataSync AWS Outposts

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

S3BucketArn

Speciifica l'ARN del bucket S3 che desideri utilizzare come posizione. (Quando crei l' DataSync attività in un secondo momento, specifichi se questa posizione è una fonte o una destinazione di trasferimento.)

Se il bucket S3 si trova su una AWS Outposts risorsa, devi specificare un punto di accesso Amazon S3. Per ulteriori informazioni, consulta Gestire l'accesso ai dati con i punti di accesso Amazon S3 nella Amazon S3 User Guide.

Tipo: stringa

Limiti di lunghezza: lunghezza massima di 268.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

Campo obbligatorio: sì

S3Config

Speciifica l'Amazon Resource Name (ARN) AWS Identity and Access Management del ruolo DataSync (IAM) utilizzato per accedere al bucket S3.

Per ulteriori informazioni, consulta Fornire l' DataSync accesso ai bucket S3.

Tipo: oggetto S3Config

Campo obbligatorio: sì

S3StorageClass

Speciifica la classe di storage che desideri che i tuoi oggetti utilizzino quando Amazon S3 è una destinazione di trasferimento.

Per i bucket in Regioni AWS, la classe di storage predefinita è. `STANDARD` Per i bucket attivi AWS Outposts, la classe di archiviazione ha come impostazione predefinita. `OUTPOSTS`

Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con i trasferimenti Amazon S3.

Tipo: stringa

Valori validi: `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

Campo obbligatorio: no

Subdirectory

Speciifica un prefisso nel bucket S3 da cui eseguire la DataSync lettura o la scrittura (a seconda che il bucket sia una posizione di origine o di destinazione).

> **Note**
>
> DataSync non può trasferire oggetti con un prefisso che inizia con una barra () `/` o include o pattern. `// /./ /../` Per esempio:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`
> - `photos/../2006/March`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: no

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse. AWS Ti consigliamo di creare almeno un'etichetta con il nome della località di trasferimento.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'ARN della posizione S3 che hai creato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Fase 1: Consenti di assumere il ruolo IAM richiesto per scrivere nel bucket

L'esempio seguente mostra la policy più semplice che concede le autorizzazioni necessarie per accedere AWS DataSync a un bucket Amazon S3 di destinazione, seguita da un ruolo IAM a cui è stata allegata `create-location-s3-iam-role` la policy.

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

```
"Role": {
        "Path": "/",
        "RoleName": "amzn-s3-demo-bucket-access-role",
        "RoleId": "role-id",
        "Arn": "arn:aws:iam::account-id:role/amzn-s3-demo-bucket-access-role",
        "CreateDate": "2018-07-27T02:49:23.117Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
```

```
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "datasync.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Fase 2: Consenti al ruolo IAM creato di scrivere nel bucket

Allega al ruolo una policy con autorizzazioni sufficienti per accedere al bucket. Un esempio di tale politica è la politica `AWSDataSyncFullAccess` gestita.

Per ulteriori informazioni, consulta AWSDataSyncFullAccessnella console IAM.

Non è necessario creare questa policy. È gestito da AWS, quindi tutto ciò che devi fare è specificare il suo ARN nel `attach-role-policy` comando.

```
IAM_POLICY_ARN='arn:aws:iam::aws:policy/AWSDataSyncFullAccess'
```

Fase 3. Crea un endpoint per un bucket Amazon S3

L'esempio seguente crea un endpoint per un bucket Amazon S3.

Quando viene creato l'endpoint S3, una risposta simile al secondo esempio seguente restituisce l'Amazon Resource Name (ARN) per la nuova posizione Amazon S3.

Richiesta di esempio

```
{
  "S3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket",
  "S3Config": {
     "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/amzn-s3-demo-bucket-access-
role",
    },
    "S3StorageClass": "STANDARD",
    "Subdirectory": "/MyFolder",
    "Tags": [
```

```
        {
           "Key": "Name",
           "Value": "s3Bucket-1"
        }
     ]
}
```

Risposta di esempio

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLocationSmb

Crea una posizione di trasferimento per un file server Server Message Block (SMB). AWS DataSync può utilizzare questa posizione come origine o destinazione per il trasferimento di dati.

Prima di iniziare, assicurati di aver compreso come DataSync accede ai file server SMB. Per ulteriori informazioni, consulta Fornire DataSync l'accesso ai file server SMB.

Sintassi della richiesta

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArns

Speciifica l' DataSync agente (o gli agenti) che possono connettersi al file server SMB. Specifichi un agente utilizzando il relativo Amazon Resource Name (ARN).

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: sì

AuthenticationType

Speciifica il protocollo di autenticazione DataSync utilizzato per connettersi al file server SMB. DataSync supporta `NTLM` (impostazione predefinita) e `KERBEROS` autenticazione.

Per ulteriori informazioni, vedere Fornire DataSync l'accesso ai file server SMB.

Tipo: stringa

Valori validi: `NTLM | KERBEROS`

Campo obbligatorio: no

DnsIpAddresses

Speciifica IPv6 gli IPv4 o gli indirizzi per i server DNS a cui appartiene il file server SMB. Questo parametro si applica solo se `AuthenticationType` è impostato su. `KERBEROS`

Se nell'ambiente sono presenti più domini, la configurazione di questo parametro assicura la DataSync connessione al file server SMB corretto.

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 2 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 7. Lunghezza massima di 39.

Modello: `\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

Campo obbligatorio: no

Domain

Specifica il nome dominio di Windows a cui appartiene il server di file SMB. Questo parametro si applica solo se `AuthenticationType` è impostato su`NTLM`.

Se nell'ambiente sono presenti più domini, la configurazione di questo parametro assicura la DataSync connessione al file server corretto.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Campo obbligatorio: no

KerberosKeytab

Speciifica il file della tabella delle chiavi Kerberos (keytab), che include le mappature tra la chiave principale Kerberos e la chiave di crittografia.

Per evitare errori di esecuzione delle attività, assicurati che il principale Kerberos utilizzato per creare il file keytab corrisponda esattamente a quello specificato. `KerberosPrincipal`

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 65536.

Campo obbligatorio: no

KerberosKrb5Conf

Specifica un file di configurazione Kerberos (`krb5.conf`) che definisce la configurazione del realm Kerberos.

Il file deve essere codificato in base 64. Se stai usando il AWS CLI, la codifica è pronta per te.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 131072.

Campo obbligatorio: no

KerberosPrincipal

Speciifica un principale Kerberos, che è un'identità nell'area di autenticazione Kerberos che dispone dell'autorizzazione ad accedere a file, cartelle e metadati dei file nel file server SMB.

Potrebbe essere simile a un principale Kerberos. `HOST/kerberosuser@MYDOMAIN.ORG`

I nomi principali distinguono tra maiuscole e minuscole. L'esecuzione dell' DataSync attività avrà esito negativo se il principale specificato per questo parametro non corrisponde esattamente al principale utilizzato per creare il file keytab.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^.+$`

Campo obbligatorio: no

MountOptions

Speciifica la versione del protocollo SMB DataSync utilizzata per accedere al file server SMB.

Tipo: oggetto SmbMountOptions

Campo obbligatorio: no

Password

Speciifica la password dell'utente che può montare il file server SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento. Questo parametro si applica solo se `AuthenticationType` è impostato su. `NTLM`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^.{0,104}$`

Campo obbligatorio: no

ServerHostname

Speciifica il nome di dominio o l'indirizzo IP (IPv4 o IPv6) del file server SMB a cui l'agente si connette DataSync .

> **Note**
>
> Se utilizzi l'autenticazione Kerberos, devi specificare un nome di dominio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Campo obbligatorio: sì

Subdirectory

Speciifica il nome della condivisione esportata dal file server SMB in cui leggerà o DataSync scriverà i dati. È possibile includere una sottodirectory nel percorso di condivisione (ad esempio,). `/path/to/subdirectory` Assicurati che anche altri client SMB della tua rete possano montare questo percorso.

Per copiare tutti i dati nella sottodirectory, DataSync devi essere in grado di montare la condivisione SMB e accedere a tutti i suoi dati. Per ulteriori informazioni, consulta Fornire DataSync l'accesso ai file server SMB.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: sì

Tags

Specifica le etichette che consentono di classificare, filtrare e cercare le risorse AWS . È consigliabile creare almeno un tag di nome per la posizione.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

User

Speciifica l'utente che può montare e accedere ai file, alle cartelle e ai metadati dei file nel file server SMB. Questo parametro si applica solo se `AuthenticationType` è impostato su. `NTLM`

Per informazioni sulla scelta di un utente con il giusto livello di accesso per il trasferimento, consulta Fornire DataSync l'accesso ai file server SMB.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "LocationArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LocationArn

L'ARN della sede SMB che hai creato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

L'esempio seguente crea una posizione per un file server SMB.

```
{
   "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"
}
```

Risposta di esempio

Una risposta restituisce l'ARN della posizione del file server SMB.

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

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateTask

Configura un'attività, che definisce dove e come vengono AWS DataSync trasferiti i dati.

Un'attività include una posizione di origine, una posizione di destinazione e opzioni di trasferimento (come limiti di larghezza di banda, pianificazione e altro).

> **Important**
>
> Se hai intenzione di trasferire dati da o verso una sede Amazon S3, consulta in che modo DataSync possono influire sui costi delle richieste S3 e sulla pagina dei DataSync prezzi prima di iniziare.

Sintassi della richiesta

```
{
   "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"
   }
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

CloudWatchLogGroupArn

Speciifica l'Amazon Resource Name (ARN) di un gruppo di log CloudWatch Amazon per il monitoraggio dell'attività.

Per le attività in modalità avanzata, non è necessario specificare nulla. DataSyncinvia automaticamente i log a un gruppo di CloudWatch log denominato`/aws/datasync`.

Per ulteriori informazioni, vedere Monitoraggio dei trasferimenti di dati con i CloudWatch registri.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 562.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

Campo obbligatorio: no

DestinationLocationArn

Specifica l'ARN della località di destinazione del trasferimento.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Excludes

Speciifica i filtri di esclusione che definiscono i file, gli oggetti e le cartelle nella posizione di origine che non si desidera DataSync trasferire. Per ulteriori informazioni ed esempi, consulta Specificare DataSync i trasferimenti utilizzando i filtri.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

Includes

Le specifiche includono i filtri che definiscono i file, gli oggetti e le cartelle che si desidera DataSync trasferire nella posizione di origine. Per ulteriori informazioni ed esempi, vedere Specificazione dei DataSync trasferimenti mediante filtri.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

ManifestConfig

Configura un manifesto, che è un elenco di file o oggetti che si desidera DataSync trasferire. Per ulteriori informazioni ed esempi di configurazione, vedere Specificazione degli elementi da DataSync trasferire utilizzando un manifesto.

Quando si utilizza questo parametro, l'identità del chiamante (il ruolo DataSync con cui si utilizza) deve disporre dell'`iam:PassRole`autorizzazione. La AWSDataSyncFullAccesspolitica include questa autorizzazione.

Tipo: oggetto ManifestConfig

Campo obbligatorio: no

Name

Specificate il nome dell'attività.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

Options

Speciifica le impostazioni dell'attività, come la conservazione dei metadati dei file, la verifica dell'integrità dei dati, tra le altre opzioni.

Tipo: oggetto Options

Campo obbligatorio: no

Schedule

Specificate una pianificazione per quando desiderate che l'attività venga eseguita. Per ulteriori informazioni, vedere Pianificazione delle attività.

Tipo: oggetto TaskSchedule

Campo obbligatorio: no

SourceLocationArn

Specifica l'ARN della posizione di origine del trasferimento.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Tags

Specificate i tag da applicare all'attività.

I tag sono coppie chiave-valore che consentono di gestire, filtrare e cercare le risorse. DataSync

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

TaskMode

Specifica una delle seguenti modalità di attività per il trasferimento dei dati:

- `ENHANCED`- Trasferisci un numero virtualmente illimitato di oggetti con prestazioni superiori rispetto alla modalità Basic. Le attività in modalità avanzata ottimizzano il processo di trasferimento dei dati elencando, preparando, trasferendo e verificando i dati in parallelo. La modalità avanzata è attualmente disponibile per i trasferimenti tra sedi Amazon S3, i trasferimenti tra Azure Blob e Amazon S3 senza un agente e i trasferimenti tra altri cloud e Amazon S3 senza agente.

  > **Note**
  >
  > Per creare un'attività in modalità avanzata, il ruolo IAM utilizzato per chiamare l'`CreateTask`operazione deve disporre dell'autorizzazione. `iam:CreateServiceLinkedRole`

- `BASIC`(impostazione predefinita): trasferisci file o oggetti tra l' AWS archiviazione e tutte le altre DataSync posizioni supportate. Le attività in modalità base sono soggette a quote sul numero di file, oggetti e directory in un set di dati. La modalità base prepara, trasferisce e verifica i dati in modo sequenziale, rendendola più lenta della modalità avanzata per la maggior parte dei carichi di lavoro.

Per ulteriori informazioni, vedere Comprensione delle differenze tra le modalità di attività.

Tipo: stringa

Valori validi: `BASIC | ENHANCED`

Campo obbligatorio: no

TaskReportConfig

Specifica come si desidera configurare un rapporto sulle attività, che fornisce informazioni dettagliate sul DataSync trasferimento. Per ulteriori informazioni, consulta Monitoraggio dei DataSync trasferimenti con i report sulle attività.

Quando si utilizza questo parametro, l'identità del chiamante (il ruolo DataSync con cui si utilizza) deve disporre dell'`iam:PassRole`autorizzazione. La AWSDataSyncFullAccesspolitica include questa autorizzazione.

Tipo: oggetto TaskReportConfig

Campo obbligatorio: no

Sintassi della risposta

```
{
   "TaskArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

TaskArn

L'Amazon Resource Name (ARN) dell'attività.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Esempio di richiesta per un'attività in modalità avanzata

L'esempio seguente crea un' DataSync attività che utilizza la modalità avanzata.

A differenza di quando si creano attività in modalità Basic, non è necessario specificare un gruppo di CloudWatch log Amazon. Con le attività in modalità avanzata, invia DataSync automaticamente i log delle attività a un gruppo di log denominato`/aws/datasync`. Se quel gruppo di log non esiste nel tuo Regione AWS, DataSync crea il gruppo di log per tuo conto quando crei l'attività.

```
{
  "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"
  }
}
```

Esempio di richiesta per un'attività in modalità Basic

L'esempio seguente crea un' DataSync attività che utilizza la modalità Basic.

```
{
```

```
    "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"
        }
    ]
}
```

Risposta di esempio

La risposta seguente include l'ARN di un'attività creata.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteAgent

Rimuove una risorsa AWS DataSync agente dal tuo Account AWS.

Tieni presente che questa operazione (che non può essere annullata) non rimuove la macchina virtuale (VM) dell'agente o l' EC2 istanza Amazon dal tuo ambiente di storage. Per i passaggi successivi, puoi eliminare la macchina virtuale o l'istanza dal tuo ambiente di storage o riutilizzarla per attivare un nuovo agente.

Sintassi della richiesta

```
{
   "AgentArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArn

L'Amazon Resource Name (ARN) dell'agente da eliminare. Utilizza l'`ListAgents`operazione per restituire un elenco di agenti per il tuo account e Regione AWS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteLocation

Elimina una risorsa relativa alla posizione di trasferimento da AWS DataSync.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

L'Amazon Resource Name (ARN) della posizione da eliminare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteTask

Elimina una risorsa dell'attività di trasferimento da AWS DataSync.

Sintassi della richiesta

```
{
   "TaskArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

TaskArn

Speciifica l'Amazon Resource Name (ARN) dell'attività che desideri eliminare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeAgent

Restituisce informazioni su un AWS DataSync agente, ad esempio il nome, il tipo di endpoint del servizio e lo stato.

Sintassi della richiesta

```
{
   "AgentArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArn

Speciifica l'Amazon Resource Name (ARN) DataSync dell'agente su cui desideri informazioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "AgentArn": "string",
   "CreationTime": number,
   "EndpointType": "string",
   "LastConnectionTime": number,
   "Name": "string",
   "Platform": {
      "Version": "string"
   },
```

```
   "PrivateLinkConfig": {
      "PrivateLinkEndpoint": "string",
      "SecurityGroupArns": [ "string" ],
      "SubnetArns": [ "string" ],
      "VpcEndpointId": "string"
   },
   "Status": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AgentArn

L'ARN dell'agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

L'ora in cui l'agente è stato attivato.

Tipo: Timestamp

EndpointType

Il tipo di endpoint di servizio a cui è connesso l'agente.

Tipo: stringa

Valori validi: `PUBLIC | PRIVATE_LINK | FIPS`

LastConnectionTime

L'ultima volta che l'agente ha comunicato con il DataSync servizio.

Tipo: Timestamp

Name

Il nome dell'agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Platform

I dettagli relativi alla piattaforma sull'agente, ad esempio il numero di versione.

Tipo: oggetto Platform

PrivateLinkConfig

La configurazione di rete utilizzata dall'agente per la connessione a un endpoint del servizio VPC.

Tipo: oggetto PrivateLinkConfig

Status

Lo stato dell'agente.

- Se lo stato è`ONLINE`, l'agente è configurato correttamente e pronto per l'uso.
- Se lo stato è`OFFLINE`, l'agente non è in contatto con l'agente DataSync da cinque minuti o più. Questo può succedere per diversi motivi. Per ulteriori informazioni, vedi Cosa devo fare se il mio agente è offline?

Tipo: stringa

Valori validi: `ONLINE | OFFLINE`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

L'esempio seguente restituisce informazioni su un agente specificato in una richiesta.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0"
}
```

Risposta di esempio

Il seguente esempio di risposta descrive un agente che utilizza un endpoint di servizio pubblico.

```
{
    "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"
    }
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationAzureBlob

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento per Microsoft Azure Blob Storage.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione di trasferimento di Azure Blob Storage.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AccessTier

Il livello di accesso in cui desideri trasferire i tuoi oggetti o file. Questo vale solo quando si utilizza la posizione come destinazione di trasferimento. Per ulteriori informazioni, consulta Livelli di accesso.

Tipo: stringa

Valori validi: `HOT | COOL | ARCHIVE`

AgentArns

Gli DataSync agenti che possono connettersi al contenitore Azure Blob Storage. ARNs

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Il metodo di autenticazione DataSync utilizzato per accedere all'archivio BLOB di Azure. DataSync può accedere all'archiviazione BLOB utilizzando una firma ad accesso condiviso (SAS).

Tipo: stringa

Valori validi: `SAS | NONE`

BlobType

Il tipo di blob che vuoi che siano i tuoi oggetti o file quando li trasferisci in Azure Blob Storage. Attualmente, supporta DataSync solo lo spostamento di dati in Azure Blob Storage come block blob. Per altre informazioni sui tipi di blob, consulta la documentazione di Azure Blob Storage.

Tipo: stringa

Valori validi: `BLOCK`

CmkSecretConfig

Descrive le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione DataSync utilizzato per accedere a una posizione di archiviazione specifica, con un segreto gestito dal cliente. AWS KMS key

Tipo: oggetto CmkSecretConfig

CreationTime

L'ora in cui è stata creata la posizione di trasferimento di Azure Blob Storage.

Tipo: Timestamp

CustomSecretConfig

Descrive le informazioni di configurazione per un segreto gestito dal cliente, ad esempio un token di autenticazione DataSync utilizzato per accedere a una posizione di archiviazione specifica, con un codice gestito dal cliente. AWS KMS key

Tipo: oggetto CustomSecretConfig

LocationArn

L'ARN della posizione di trasferimento di Azure Blob Storage.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URL del contenitore Azure Blob Storage coinvolto nel trasferimento.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

Descrive le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione DataSync utilizzato per accedere a una posizione di archiviazione specifica. DataSync utilizza la chiave KMS AWS gestita di default per crittografare questo segreto. AWS Secrets Manager

Tipo: oggetto ManagedSecretConfig

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationEfs

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento per un file system Amazon EFS.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

L'Amazon Resource Name (ARN) della posizione del file system Amazon EFS su cui desideri informazioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "AccessPointArn": "string",
   "CreationTime": number,
   "Ec2Config": {
      "SecurityGroupArns": [ "string" ],
      "SubnetArn": "string"
   },
   "FileSystemAccessRoleArn": "string",
```

```
   "InTransitEncryption": "string",
   "LocationArn": "string",
   "LocationUri": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AccessPointArn

L'ARN del punto di accesso DataSync utilizzato per accedere al file system Amazon EFS.

Per ulteriori informazioni, consulta Accesso ai file system con restrizioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

CreationTime

L'ora in cui è stata creata la posizione.

Tipo: Timestamp

Ec2Config

La sottorete e i gruppi di sicurezza AWS DataSync utilizzati per connettersi a uno degli obiettivi di montaggio del file system Amazon EFS.

Tipo: oggetto Ec2Config

FileSystemAccessRoleArn

Il ruolo AWS Identity and Access Management (IAM) che consente di accedere DataSync al file system Amazon EFS.

Per ulteriori informazioni, consulta Creazione di un ruolo DataSync IAM per l'accesso al file system.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

InTransitEncryption

Indica se DataSync utilizza la crittografia Transport Layer Security (TLS) per il trasferimento di dati da o verso il file system Amazon EFS.

Tipo: stringa

Valori validi: `NONE | TLS1_2`

LocationArn

L'ARN della posizione del file system Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URL della posizione del file system Amazon EFS.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

L'esempio seguente mostra come ottenere informazioni su una posizione specifica del file system Amazon EFS.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-12abcdef012345678"
}
```

Risposta di esempio

L'esempio seguente restituisce i dettagli sulla posizione di un file system Amazon EFS.

```
{
    "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/"
}
```

Esempio di risposta: descrizione di una posizione per un file system Amazon EFS con restrizioni

L'esempio seguente restituisce i dettagli sulla posizione di un file system Amazon EFS con accesso limitato`AccessPointArn`, inclusi gli `InTransitEncryption` elementi`FileSystemAccessRoleArn`, e.

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

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationFsxLustre

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento FSx per un file system Amazon for Lustre.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

L'Amazon Resource Name (ARN) della posizione FSx for Lustre da descrivere.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "SecurityGroupArns": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui è stata creata la sede FSx for Lustre.

Tipo: Timestamp

LocationArn

L'Amazon Resource Name (ARN) della posizione FSx for Lustre descritta.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI della posizione FSx for Lustre descritta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

Amazon Resource Names (ARNs) dei gruppi di sicurezza configurati per il file system FSx for Lustre.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationFsxOntap

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento FSx per un file system Amazon for NetApp ONTAP.

> **Note**
>
> Se la tua posizione utilizza SMB, l'`DescribeLocationFsxOntap`operazione non restituisce effettivamente un. `Password`

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione FSx del file system for ONTAP su cui desideri informazioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui è stata creata la posizione.

Tipo: Timestamp

FsxFilesystemArn

L'ARN del file system FSx for ONTAP.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

LocationArn

L'ARN della posizione del file system FSx for ONTAP.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'Uniform Resource Identifier (URI) della posizione del file FSx system ONTAP.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

Speciifica il protocollo di trasferimento dati AWS DataSync utilizzato per accedere al tuo FSx file system Amazon.

Tipo: oggetto FsxProtocol

SecurityGroupArns

I gruppi di sicurezza DataSync utilizzati per accedere al file system FSx for ONTAP.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

StorageVirtualMachineArn

L'ARN della macchina virtuale di archiviazione (SVM) sul file system FSx for ONTAP su cui stai copiando i dati da o verso cui stai copiando i dati.

Tipo: stringa

Limiti di lunghezza: lunghezza massima di 162.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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,}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationFsxOpenZfs

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento FSx per un file system Amazon for OpenZFS.

> **Note**
>
> Gli elementi di risposta correlati a SMB non sono supportati dall'`DescribeLocationFsxOpenZfs`operazione.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

L'Amazon Resource Name (ARN) della posizione FSx per OpenZFS da descrivere.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
```

```
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "SecurityGroupArns": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui è stata creata la FSx posizione for OpenZFS.

Tipo: Timestamp

LocationArn

L'ARN della posizione FSx per OpenZFS descritta.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'Uniform Resource Identifier (URI) della posizione FSx per OpenZFS descritta.

Esempio: `fsxz://us-west-2.fs-1234567890abcdef02/fsx/folderA/folder`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

Il tipo di protocollo AWS DataSync utilizzato per accedere al file system.

Tipo: oggetto FsxProtocol

SecurityGroupArns

I gruppi ARNs di sicurezza configurati per il file system FSx per OpenZFS.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationFsxWindows

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento FSx per un file system Amazon for Windows File Server.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione FSx del file server per Windows.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "CreationTime": number,
   "Domain": "string",
   "LocationArn": "string",
   "LocationUri": "string",
   "SecurityGroupArns": [ "string" ],
   "User": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui è stata FSx creata la posizione per Windows File Server.

Tipo: Timestamp

Domain

Il nome del dominio Microsoft Active Directory a cui appartiene il file system FSx for Windows File Server.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

LocationArn

L'ARN della posizione del file server FSx per Windows.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'Uniform Resource Identifier (URI) della posizione FSx per Windows File Server.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

I gruppi ARNs di EC2 sicurezza di Amazon che forniscono l'accesso alla sottorete preferita del tuo file system.

Per informazioni sulla configurazione dei gruppi di sicurezza per l'accesso al file system, consulta la Amazon FSx for Windows File Server User Guide.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

User

L'utente con le autorizzazioni per montare e accedere al file system FSx per Windows File Server.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationHdfs

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento per un Hadoop Distributed File System (HDFS).

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione HDFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AgentArns

Gli DataSync agenti che possono connettersi al tuo cluster HDFS. ARNs

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Il tipo di autenticazione utilizzato per determinare l'identità dell'utente.

Tipo: stringa

Valori validi: `SIMPLE | KERBEROS`

BlockSize

La dimensione dei blocchi di dati da scrivere nel cluster HDFS.

Tipo: integer

Intervallo valido: valore minimo di 1048576. Valore massimo di 1073741824.

CreationTime

L'ora in cui è stata creata la posizione HDFS.

Tipo: Timestamp

KerberosPrincipal

Il principale Kerberos con accesso ai file e alle cartelle sul cluster HDFS. Questo parametro viene utilizzato se `AuthenticationType` è definito come`KERBEROS`.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^.+$`

KmsKeyProviderUri

L'URI del Key Management Server (KMS) del cluster HDFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `^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

L'ARN della posizione HDFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI della posizione HDFS.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

NameNodes

Il NameNode che gestisce lo spazio dei nomi HDFS.

Tipo: matrice di oggetti HdfsNameNode

Membri dell'array: numero minimo di 1 elemento.

QopConfiguration

La configurazione Quality of Protection (QOP), che specifica la Remote Procedure Call (RPC) e le impostazioni di protezione del trasferimento dati configurate sul cluster HDFS.

Tipo: oggetto QopConfiguration

ReplicationFactor

Il numero DataNodes su cui replicare i dati durante la scrittura sul cluster HDFS.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 512.

SimpleUser

Il nome utente per identificare il client sul sistema operativo host. Questo parametro viene utilizzato se `AuthenticationType` è definito come`SIMPLE`.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationNfs

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento per un file server NFS (Network File System).

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione NFS su cui desideri informazioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
```

```
    }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui è stata creata la posizione NFS.

Tipo: Timestamp

LocationArn

L'ARN della posizione NFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI della posizione NFS.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

MountOptions

Le opzioni di montaggio DataSync utilizzate per montare il file server NFS.

Tipo: oggetto NfsMountOptions

OnPremConfig

Gli AWS DataSync agenti che possono connettersi al file server Network File System (NFS).

Tipo: oggetto OnPremConfig

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente restituisce informazioni sulla posizione NFS specificata nella richiesta di esempio.

Richiesta di esempio

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

Esempio

Questo esempio illustra un utilizzo di. DescribeLocationNfs

Risposta di esempio

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

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationObjectStorage

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento per un sistema di storage di oggetti.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione del sistema di storage degli oggetti.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AccessKey

La chiave di accesso (ad esempio, un nome utente) necessaria per l'autenticazione con il sistema di storage di oggetti.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `^.*$`

AgentArns

Gli DataSync agenti che possono connettersi al sistema di storage degli oggetti. ARNs

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CmkSecretConfig

Descrive le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione o un set di credenziali da DataSync utilizzare per accedere a una posizione di trasferimento specifica, e un segreto gestito dal cliente. AWS KMS key

Tipo: oggetto CmkSecretConfig

CreationTime

L'ora in cui è stata creata la posizione.

Tipo: Timestamp

CustomSecretConfig

Descrive le informazioni di configurazione per un segreto gestito dal cliente, ad esempio un token di autenticazione o un set di credenziali DataSync utilizzato per accedere a una posizione di trasferimento specifica, e un segreto gestito dal cliente. AWS KMS key

Tipo: oggetto CustomSecretConfig

LocationArn

L'ARN della posizione del sistema di storage degli oggetti.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI della posizione del sistema di storage degli oggetti.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

Descrive le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione o un set di credenziali da DataSync utilizzare per accedere a una posizione di

trasferimento specifica. DataSync utilizza la chiave KMS AWS gestita di default per crittografare questo segreto. AWS Secrets Manager

Tipo: oggetto ManagedSecretConfig

ServerCertificate

La catena di certificati DataSync per l'autenticazione con il sistema di archiviazione degli oggetti se il sistema utilizza un'autorità di certificazione (CA) privata o autofirmata.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 32768.

ServerPort

La porta su cui il server di archiviazione degli oggetti accetta il traffico di rete in entrata (ad esempio, la porta 443).

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 65536.

ServerProtocol

Il protocollo utilizzato dal sistema di storage degli oggetti per comunicare.

Tipo: stringa

Valori validi: `HTTPS | HTTP`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationS3

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento per un bucket S3.

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione Amazon S3.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "AgentArns": [ "string" ],
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
```

```
   "S3StorageClass": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AgentArns

Gli DataSync agenti distribuiti sul tuo Outpost quando utilizzi Amazon S3 su Outposts. ARNs

Per ulteriori informazioni, consulta Deploy your agent on. DataSync AWS Outposts

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

L'ora in cui è stata creata la sede Amazon S3.

Tipo: Timestamp

LocationArn

L'ARN della sede Amazon S3.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URL della posizione Amazon S3 descritta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

S3Config

Speciifica l'Amazon Resource Name (ARN) AWS Identity and Access Management del ruolo DataSync (IAM) utilizzato per accedere al bucket S3.

Per ulteriori informazioni, consulta Fornire l' DataSync accesso ai bucket S3.

Tipo: oggetto S3Config

S3StorageClass

Quando Amazon S3 è una posizione di destinazione, questa è la classe di storage che hai scelto per i tuoi oggetti.

Alcune classi di storage hanno comportamenti che possono influire sui costi di storage di Amazon S3. Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con i trasferimenti Amazon S3.

Tipo: stringa

Valori validi: `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente restituisce informazioni sulla posizione Amazon S3 specificata nella richiesta di esempio.

Richiesta di esempio

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

Esempio

Questo esempio illustra un utilizzo di DescribeLocation S3.

Risposta di esempio

```
{
   "CreationTime": 1532660733.39,
   "LocationArn": "arn:aws:datasync: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"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLocationSmb

Fornisce dettagli su come è configurata una posizione di AWS DataSync trasferimento per un file server Server Message Block (SMB).

Sintassi della richiesta

```
{
   "LocationArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della sede SMB su cui desideri informazioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "CreationTime": number,
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosPrincipal": "string",
   "LocationArn": "string",
```

```
   "LocationUri": "string",
   "MountOptions": {
      "Version": "string"
   },
   "User": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AgentArns

Gli DataSync agenti che possono connettersi al tuo file server SMB. ARNs

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Il protocollo di autenticazione DataSync utilizzato per connettersi al file server SMB.

Tipo: stringa

Valori validi: `NTLM | KERBEROS`

CreationTime

L'ora in cui è stata creata la sede SMB.

Tipo: Timestamp

DnsIpAddresses

IPv6 Gli indirizzi IPv4 o dei server DNS a cui appartiene il file server SMB. Questo elemento si applica solo se `AuthenticationType` è impostato su. `KERBEROS`

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 2 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 7. Lunghezza massima di 39.

Modello: `\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

Il nome del dominio Windows a cui appartiene il file server SMB. Questo elemento si applica solo se `AuthenticationType` è impostato su. `NTLM`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

KerberosPrincipal

Il principale Kerberos che dispone dell'autorizzazione per accedere a file, cartelle e metadati dei file nel file server SMB.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^.+$`

LocationArn

L'ARN della sede SMB.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI della sede SMB.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

MountOptions

La versione del protocollo SMB DataSync utilizzata per accedere al file server SMB.

Tipo: oggetto SmbMountOptions

User

L'utente che può montare e accedere a file, cartelle e metadati dei file nel file server SMB. Questo elemento si applica solo se `AuthenticationType` è impostato su. `NTLM`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Esempio

Questo esempio illustra un utilizzo di. DescribeLocationSmb

Richiesta di esempio

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

Esempio

Questo esempio illustra un utilizzo di. DescribeLocationSmb

Risposta di esempio

```
{
   "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"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeTask

Fornisce informazioni su un'attività, che definisce dove e come vengono AWS DataSync trasferiti i dati.

Sintassi della richiesta

```
{
   "TaskArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

TaskArn

Specifica l'Amazon Resource Name (ARN) dell'attività di trasferimento su cui desideri informazioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CloudWatchLogGroupArn

L'Amazon Resource Name (ARN) di un gruppo di CloudWatch log Amazon per il monitoraggio delle tue attività.

Per ulteriori informazioni, consulta Monitoraggio dei trasferimenti di dati con CloudWatch Logs.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 562.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

CreationTime

L'ora in cui è stata creata l'attività.

Tipo: Timestamp

CurrentTaskExecutionArn

L'ARN dell'esecuzione dell'attività più recente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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

L'ARN della località di destinazione del trasferimento.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

DestinationNetworkInterfaceArns

Le interfacce ARNs di rete DataSync create per la località di destinazione.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

ErrorCode

Se c'è un problema con la tua attività, puoi utilizzare il codice di errore per aiutarti a risolverlo. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi ai DataSync trasferimenti.

Tipo: stringa

ErrorDetail

Se c'è un problema con la tua attività, puoi utilizzare i dettagli dell'errore per aiutarti a risolverlo. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi ai DataSync trasferimenti.

Tipo: stringa

Excludes

I filtri di esclusione che definiscono i file, gli oggetti e le cartelle nella posizione di origine che non desideri DataSync trasferire. Per ulteriori informazioni ed esempi, consulta Specificare i DataSync trasferimenti utilizzando i filtri.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Includes

Includono filtri che definiscono i file, gli oggetti e le cartelle che si desidera DataSync trasferire nella posizione di origine. Per ulteriori informazioni ed esempi, consulta Specificare i DataSync trasferimenti utilizzando i filtri.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

ManifestConfig

La configurazione del manifesto che elenca i file o gli oggetti che si desidera DataSync trasferire. Per ulteriori informazioni, vedere Specificazione dei DataSync trasferimenti utilizzando un manifesto.

Tipo: oggetto ManifestConfig

Name

Il nome dell'attività.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Options

Le impostazioni dell'attività. Ad esempio, quali metadati dei file vengono conservati, come viene verificata l'integrità dei dati al termine del trasferimento, limiti di larghezza di banda, tra le altre opzioni.

Tipo: oggetto Options

Schedule

La pianificazione del momento in cui desideri che l'attività venga eseguita. Per ulteriori informazioni, vedere Pianificazione delle attività.

Tipo: oggetto TaskSchedule

ScheduleDetails

I dettagli sulla pianificazione delle attività.

Tipo: oggetto TaskScheduleDetails

SourceLocationArn

L'ARN della posizione di origine del trasferimento.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

SourceNetworkInterfaceArns

Le interfacce ARNs di rete DataSync create per la posizione di origine.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

Status

Lo stato dell'attività. Per informazioni sul significato di ogni stato, consulta Stati delle attività.

Tipo: stringa

Valori validi: `AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE`

TaskArn

L'ARN della tua attività.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

TaskMode

La modalità di attività che stai utilizzando. Per ulteriori informazioni, vedere Scelta di una modalità di operazione per il trasferimento dei dati.

Tipo: stringa

Valori validi: `BASIC | ENHANCED`

TaskReportConfig

La configurazione del rapporto sulle attività, che fornisce informazioni dettagliate sul DataSync trasferimento. Per ulteriori informazioni, consulta Monitoraggio dei DataSync trasferimenti con i report sulle attività.

Tipo: oggetto TaskReportConfig

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

L'esempio seguente specifica l'ARN di DataSync un'attività su cui ottenere informazioni.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Risposta di esempio

L'esempio seguente mostra una `DescribeTask` risposta.

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

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeTaskExecution

Fornisce informazioni sull'esecuzione dell' AWS DataSync attività. È possibile utilizzare questa operazione per monitorare lo stato di avanzamento di un trasferimento di dati in corso o verificare i risultati del trasferimento.

> **Note**
>
> Alcuni elementi di `DescribeTaskExecution` risposta sono rilevanti solo per una modalità di operazione specifica. Per informazioni, vedere Comprensione delle differenze tra le modalità di attività e Comprensione dei contatori delle prestazioni del trasferimento dati.

Sintassi della richiesta

```
{
   "TaskExecutionArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

TaskExecutionArn

Specifica l'Amazon Resource Name (ARN) dell'esecuzione dell'attività su cui desideri informazioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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}$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "BytesCompressed": number,
   "BytesTransferred": number,
   "BytesWritten": number,
   "EndTime": number,
   "EstimatedBytesToTransfer": number,
   "EstimatedFilesToDelete": number,
   "EstimatedFilesToTransfer": 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,
   "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"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BytesCompressed

Il numero di byte fisici che vengono DataSync trasferiti sulla rete dopo la compressione (se la compressione è possibile). Questo numero è in genere inferiore BytesTransferreda quello a meno che i dati non siano comprimibili.

Tipo: long

BytesTransferred

Il numero di byte DataSync inviati alla rete prima della compressione (se la compressione è possibile). Per il numero di byte trasferiti sulla rete, vedere. BytesCompressed

Tipo: long

BytesWritten

Il numero di byte logici DataSync effettivamente scritti nella posizione di destinazione.

Tipo: long

EndTime

L'ora in cui termina l'operazione di trasferimento.

Tipo: Timestamp

EstimatedBytesToTransfer

Il numero di byte logici che DataSync prevede di scrivere nella posizione di destinazione.

Tipo: long

EstimatedFilesToDelete

Il numero di file, oggetti e directory che DataSync prevede di eliminare nella posizione di destinazione. Se non configuri l'attività per eliminare i dati nella destinazione che non si trovano nell'origine, il valore è sempre. `0`

Tipo: long

EstimatedFilesToTransfer

Il numero di file, oggetti e directory che DataSync prevede di trasferire sulla rete. Questo valore viene calcolato durante la DataSync preparazione del trasferimento.

Il modo in cui viene calcolato dipende principalmente dalla configurazione della modalità di trasferimento dell'attività:

- Se `TranserMode` è impostato su `CHANGED` - Il calcolo si basa sul confronto del contenuto delle posizioni di origine e di destinazione e sulla determinazione della differenza da trasferire. La differenza può includere:

- Tutto ciò che viene aggiunto o modificato nella posizione di origine.
- Tutto ciò che si trova in entrambe le posizioni e viene modificato nella destinazione dopo un trasferimento iniziale (a meno che non OverwriteModesia impostato su`NEVER`).
- (Solo modalità attività di base) Il numero di elementi che DataSync prevede di eliminare (se PreserveDeletedFilesè impostato su`REMOVE`).

- Se `TranserMode` è impostato su `ALL` - Il calcolo si basa solo sugli elementi DataSync trovati nella posizione di origine.

Tipo: long

Excludes

Un elenco di regole di filtro che escludono dati specifici durante il trasferimento. Per ulteriori informazioni ed esempi, consulta Filtraggio dei dati trasferiti da DataSync.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

FilesDeleted

Il numero di file, oggetti e directory DataSync effettivamente eliminati nella posizione di destinazione. Se non configuri l'attività per eliminare i dati nella destinazione che non si trovano nell'origine, il valore è sempre. `0`

Tipo: long

FilesFailed

Il numero di oggetti che DataSync non vengono preparati, trasferiti, verificati ed eliminati durante l'esecuzione dell'attività.

> **Note**
>
> Si applica solo alle attività in modalità Avanzata.

Tipo: oggetto TaskExecutionFilesFailedDetail

FilesListed

Il numero di oggetti che DataSync si trovano nelle tue posizioni.

> **Note**
>
> Si applica solo alle attività in modalità Avanzata.

Tipo: oggetto TaskExecutionFilesListedDetail

FilesPrepared

Il numero di oggetti che DataSync tenteranno di trasferire dopo aver confrontato le posizioni di origine e di destinazione.

> **Note**
>
> Si applica solo alle attività in modalità Avanzata.

Questo contatore non è applicabile se si configura l'attività per trasferire tutti i dati. In questo scenario, DataSync copia tutto dall'origine alla destinazione senza confrontare le differenze tra le posizioni.

Tipo: long

FilesSkipped

Il numero di file, oggetti e directory che vengono DataSync ignorati durante il trasferimento.

Tipo: long

FilesTransferred

Il numero di file, oggetti e directory DataSync effettivamente trasferiti sulla rete. Questo valore viene aggiornato periodicamente durante l'esecuzione dell'attività quando qualcosa viene letto dall'origine e inviato in rete.

Se DataSync non riesce a trasferire qualcosa, questo valore può essere inferiore a`EstimatedFilesToTransfer`. In alcuni casi, questo valore può anche essere maggiore di`EstimatedFilesToTransfer`. Questo elemento è specifico dell'implementazione per alcuni tipi di posizione, quindi non utilizzatelo come indicazione esatta di ciò che viene trasferito o per monitorare l'esecuzione delle attività.

Tipo: long

FilesVerified

Il numero di file, oggetti e directory che DataSync viene verificato durante il trasferimento.

> **Note**
>
> Quando configuri l'attività in modo da verificare solo i dati trasferiti, DataSync non verifica le directory in alcune situazioni o i file che non vengono trasferiti.

Tipo: long

Includes

Un elenco di regole di filtro che includono dati specifici durante il trasferimento. Per ulteriori informazioni ed esempi, consulta Filtraggio dei dati trasferiti da DataSync.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

LaunchTime

L'ora in cui inizia effettivamente l'esecuzione dell'attività. Per le attività non in coda, `LaunchTime` e in genere `StartTime` sono le stesse. Per le attività in coda, in genere `LaunchTime` è successivo rispetto al momento in cui le attività precedentemente `StartTime` accodate devono terminare l'esecuzione prima che possano iniziare le nuove attività.

Tipo: Timestamp

ManifestConfig

La configurazione del manifesto che elenca i file o gli oggetti da trasferire. Per ulteriori informazioni, vedete Specificare quali DataSync trasferimenti utilizzando un manifesto.

Tipo: oggetto ManifestConfig

Options

Indica come è configurata l'attività di trasferimento. Queste opzioni includono la modalità DataSync di gestione dei file, degli oggetti e dei metadati associati durante il trasferimento. Puoi anche specificare come verificare l'integrità dei dati, impostare limiti di larghezza di banda per l'attività, tra le altre opzioni.

Ogni opzione ha un valore predefinito. A meno che non sia necessario, non è necessario configurare alcuna opzione prima di chiamare StartTaskExecution.

È inoltre possibile sovrascrivere le opzioni dell'attività per ogni esecuzione di attività. Ad esempio, potresti voler modificare il valore `LogLevel` per una singola esecuzione.

Tipo: oggetto Options

ReportResult

Indica se è stato DataSync generato un rapporto completo sulle attività per il trasferimento.

Tipo: oggetto ReportResult

Result

Il risultato dell'esecuzione dell'attività.

Tipo: oggetto TaskExecutionResultDetail

StartTime

L'ora in cui DataSync viene inviata la richiesta per avviare l'esecuzione dell'attività. Per le attività non in coda, `LaunchTime` e in genere `StartTime` sono le stesse. Per le attività in coda, in genere `LaunchTime` è successivo rispetto al momento in cui le attività precedentemente `StartTime` accodate devono terminare l'esecuzione prima che possano iniziare le nuove attività.

Tipo: Timestamp

Status

Lo stato dell'esecuzione dell'attività.

Per informazioni dettagliate sugli stati di esecuzione delle attività, vedere Stati di esecuzione delle attività.

Tipo: stringa

Valori validi: `QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR`

TaskExecutionArn

L'ARN dell'esecuzione dell'attività su cui volevi informazioni. `TaskExecutionArn`è gerarchico e include `TaskArn` l'operazione che è stata eseguita.

Ad esempio, un `TaskExecution` valore con ARN ha `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2/execution/exec-08ef1e88ec491019b` eseguito l'operazione con l'ARN. `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2`

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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

La modalità di attività che stai utilizzando. Per ulteriori informazioni, vedere Scelta di una modalità di operazione per il trasferimento dei dati.

Tipo: stringa

Valori validi: `BASIC | ENHANCED`

TaskReportConfig

La configurazione del rapporto sulle attività, che fornisce informazioni dettagliate sul DataSync trasferimento. Per ulteriori informazioni, vedere Creazione di un rapporto sulle attività.

Tipo: oggetto TaskReportConfig

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

Questo esempio illustra una richiesta. `DescribeTaskExecution`

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1"
}
```

Esempio di risposta 1 per l'esecuzione di un'attività in modalità avanzata

L'esempio seguente descrive un'esecuzione di DataSync attività che utilizza la modalità avanzata. L'esecuzione trasferisce anche dati specifici utilizzando i filtri di esclusione e inclusione.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/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,
    "EstimatedBytesToTransfer": 30,
    "FilesTransferred": 7,
    "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
    }
}
```

Sample Response 2 per un'esecuzione di attività in modalità avanzata

L'esempio seguente descrive l'esecuzione di un'altra DataSync attività che utilizza la modalità Enhanced. In questa situazione, l'esecuzione consiste nel trasferire dati specifici utilizzando un manifesto anziché filtri.

```
{
```

```
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/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,
    "EstimatedBytesToTransfer": 6,
    "FilesTransferred": 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": "SUCCESSES_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
    }
```

```
}
```

Esempio di risposta per l'esecuzione di un task in modalità Basic

L'esempio seguente descrive l'esecuzione di un' DataSync attività che utilizza la modalità Basic.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/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": "SUCCESSES_AND_ERRORS"
            },
            "Transferred": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Verified": {
                "ReportLevel": "ERRORS_ONLY"
            }
        },
        "ReportLevel": "ERRORS_ONLY"
    }
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListAgents

Restituisce un elenco di AWS DataSync agenti che appartengono Account AWS a uno dei Regione AWS specificati nella richiesta.

Con l'impaginazione, è possibile ridurre il numero di agenti restituiti in una risposta. Se in una risposta viene visualizzato un elenco troncato di agenti, la risposta contiene un marker che è possibile specificare nella richiesta successiva per recuperare la pagina successiva di agenti.

`ListAgents`alla fine è coerente. Ciò significa che il risultato dell'esecuzione dell'operazione potrebbe non rispecchiare la creazione o l'eliminazione di un agente da parte dell'utente. Ad esempio, se si crea un agente con CreateAgente poi lo si esegue immediatamente`ListAgents`, tale agente potrebbe non comparire immediatamente nell'elenco. In situazioni come questa, puoi sempre confermare se un agente è stato creato (o eliminato) utilizzando DescribeAgent.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Speciifica il numero massimo di DataSync agenti da elencare in una risposta. Per impostazione predefinita, una risposta mostra un massimo di 100 agenti.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 100.

Campo obbligatorio: no

NextToken

Specifica una stringa opaca che indica la posizione in cui iniziare l'elenco successivo di risultati nella risposta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "Agents": [
      {
         "AgentArn": "string",
         "Name": "string",
         "Platform": {
            "Version": "string"
         },
         "Status": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Agents

Un elenco degli DataSync agenti presenti nel tuo account come Regione AWS specificato Account AWS nella richiesta. L'elenco è ordinato in base agli Amazon Resource Names () ARNs degli agenti.

Tipo: matrice di oggetti AgentListEntry

NextToken

La stringa opaca che indica la posizione in cui iniziare l'elenco successivo di risultati nella risposta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListLocations

Restituisce un elenco di posizioni di origine e destinazione.

Se hai più sedi di quelle restituite in una risposta (ovvero, la risposta restituisce solo un elenco troncato dei tuoi agenti), la risposta contiene un token che puoi specificare nella tua richiesta successiva per recuperare la pagina successiva di sedi.

Sintassi della richiesta

```
{
   "Filters": [
      {
         "Name": "string",
         "Operator": "string",
         "Values": [ "string" ]
      }
   ],
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Filters

Puoi utilizzare i filtri API per restringere l'elenco delle risorse restituite da. `ListLocations` Ad esempio, per recuperare tutte le attività in una posizione di origine specifica, è possibile utilizzare `ListLocations` with filter name `LocationType S3` and`Operator Equals`.

Tipo: matrice di oggetti LocationFilter

Campo obbligatorio: no

MaxResults

Il numero massimo di posizioni da restituire.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 100.

Campo obbligatorio: no

NextToken

Una stringa opaca che indica la posizione da cui iniziare il successivo elenco di posizioni.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "Locations": [
      {
         "LocationArn": "string",
         "LocationUri": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Locations

Un array che contiene un elenco di posizioni.

Tipo: matrice di oggetti LocationListEntry

NextToken

Una stringa opaca che indica la posizione da cui iniziare a restituire l'elenco successivo di posizioni.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListTagsForResource

Restituisce tutti i tag associati a una AWS risorsa.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ResourceArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Specificare il numero di risultati che si desidera ottenere nella risposta.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 100.

Campo obbligatorio: no

NextToken

Specifica una stringa opaca che indica la posizione in cui iniziare l'elenco successivo di risultati nella risposta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Campo obbligatorio: no

ResourceArn

Specifica l'Amazon Resource Name (ARN) della risorsa su cui desideri inserire le informazioni relative ai tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})(/execution/exec-[a-f0-9]{17})?$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

La stringa opaca che indica la posizione in cui iniziare il successivo elenco di risultati nella risposta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Tags

Una matrice di tag applicata alla risorsa specificata.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 55 elementi.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListTaskExecutions

Restituisce un elenco di esecuzioni per un'attività di AWS DataSync trasferimento.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "TaskArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Specificate il numero di risultati che desiderate ottenere nella risposta.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 100.

Campo obbligatorio: no

NextToken

Specifica una stringa opaca che indica la posizione da cui iniziare il successivo elenco di risultati nella risposta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Campo obbligatorio: no

TaskArn

Specifica l'Amazon Resource Name (ARN) dell'attività per la quale desideri informazioni sull'esecuzione.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "NextToken": "string",
   "TaskExecutions": [
      {
         "Status": "string",
         "TaskExecutionArn": "string",
         "TaskMode": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

La stringa opaca che indica la posizione da cui iniziare il successivo elenco di risultati nella risposta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

TaskExecutions

Un elenco delle esecuzioni dell'attività.

Tipo: matrice di oggetti TaskExecutionListEntry

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListTasks

Restituisce un elenco delle AWS DataSync attività che hai creato.

Sintassi della richiesta

```
{
   "Filters": [
      {
         "Name": "string",
         "Operator": "string",
         "Values": [ "string" ]
      }
   ],
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Filters

Puoi utilizzare i filtri API per restringere l'elenco delle risorse restituite da`ListTasks`. Ad esempio, per recuperare tutte le attività su una posizione di origine specifica, è possibile utilizzare `ListTasks` con il nome del filtro `LocationId` e `Operator Equals` con l'ARN per la posizione.

Tipo: matrice di oggetti TaskFilter

Campo obbligatorio: no

MaxResults

Il numero massimo di attività da restituire.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 100.

Campo obbligatorio: no

NextToken

Una stringa opaca che indica la posizione da cui iniziare l'elenco successivo di attività.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "NextToken": "string",
   "Tasks": [
      {
         "Name": "string",
         "Status": "string",
         "TaskArn": "string",
         "TaskMode": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Una stringa opaca che indica la posizione da cui iniziare a restituire l'elenco successivo di attività.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 65535.

Modello: `[a-zA-Z0-9=_-]+`

Tasks

Un elenco di tutte le attività restituite.

Tipo: matrice di oggetti TaskListEntry

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartTaskExecution

Avvia un'operazione AWS DataSync di trasferimento. Per ogni attività, è possibile eseguire una sola operazione alla volta.

L'esecuzione di un'attività prevede diversi passaggi. Per ulteriori informazioni, vedere Stati di esecuzione delle attività.

> **Important**
>
> Se hai intenzione di trasferire dati da o verso una sede Amazon S3, consulta in che modo DataSync possono influire sui costi delle richieste S3 e sulla pagina dei DataSync prezzi prima di iniziare.

Sintassi della richiesta

```
{
   "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"
      }
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Excludes

Specifica un elenco di regole di filtro che determina quali file escludere da un'attività. L'elenco contiene una singola stringa di filtro costituita dai modelli da escludere. I modelli sono delimitati da "|" (cioè una barra verticale), ad esempio: `"/folder1|/folder2"`.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

Includes

Specifica un elenco di regole di filtro che determina quali file includere durante l'esecuzione di un'attività. Il modello deve contenere una singola stringa di filtro costituita dai modelli da includere. I modelli sono delimitati da "|" (cioè una barra verticale), ad esempio: `"/folder1|/folder2"`.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

ManifestConfig

Configura un manifesto, che è un elenco di file o oggetti che si desidera DataSync trasferire. Per ulteriori informazioni ed esempi di configurazione, vedere Specificazione degli elementi da DataSync trasferire utilizzando un manifesto.

Quando si utilizza questo parametro, l'identità del chiamante (il ruolo DataSync con cui si utilizza) deve disporre dell'`iam:PassRole`autorizzazione. La AWSDataSyncFullAccesspolitica include questa autorizzazione.

Per rimuovere una configurazione del manifesto, specificate questo parametro con un valore vuoto.

Tipo: oggetto ManifestConfig

Campo obbligatorio: no

OverrideOptions

Indica come è configurata l'attività di trasferimento. Queste opzioni includono la modalità DataSync di gestione dei file, degli oggetti e dei metadati associati durante il trasferimento. Puoi anche specificare come verificare l'integrità dei dati, impostare limiti di larghezza di banda per l'attività, tra le altre opzioni.

Ogni opzione ha un valore predefinito. A meno che non sia necessario, non è necessario configurare alcuna opzione prima di chiamare StartTaskExecution.

È inoltre possibile sovrascrivere le opzioni dell'attività per ogni esecuzione di attività. Ad esempio, potresti voler modificare il valore `LogLevel` per una singola esecuzione.

Tipo: oggetto Options

Campo obbligatorio: no

Tags

Speciifica i tag da applicare all'Amazon Resource Name (ARN) che rappresenta l'esecuzione dell'attività.

I tag sono coppie chiave-valore che ti aiutano a gestire, filtrare e cercare le tue risorse. DataSync

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: no

TaskArn

Speciifica l'Amazon Resource Name (ARN) dell'attività che desideri avviare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Campo obbligatorio: sì

TaskReportConfig

Specifica come desideri configurare un report sulle attività, che fornisce informazioni dettagliate sul trasferimento. DataSync Per ulteriori informazioni, consulta Monitoraggio dei DataSync trasferimenti con i report sulle attività.

Quando si utilizza questo parametro, l'identità del chiamante (il ruolo DataSync con cui si utilizza) deve disporre dell'`iam:PassRole`autorizzazione. La AWSDataSyncFullAccesspolitica include questa autorizzazione.

Per rimuovere la configurazione di un report di attività, specificate questo parametro come vuoto.

Tipo: oggetto TaskReportConfig

Campo obbligatorio: no

Sintassi della risposta

```
{
   "TaskExecutionArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

TaskExecutionArn

L'ARN dell'esecuzione dell'attività in esecuzione.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Esempi

Richiesta di esempio

L'esempio seguente avvia l'esecuzione di un'attività utilizzando le opzioni predefinite per l'attività specificata.

```
{
    "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"
}
```

Risposta di esempio

Questo esempio illustra un utilizzo di. StartTaskExecution

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

TagResource

Applica un tag a una AWS risorsa. I tag sono coppie chiave-valore che possono aiutarti a gestire, filtrare e cercare le tue risorse.

Questi includono AWS DataSync risorse, come ubicazioni, attività ed esecuzioni di attività.

Sintassi della richiesta

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ResourceArn

Speciifica l'Amazon Resource Name (ARN) della risorsa a cui applicare il tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})(/execution/exec-[a-f0-9]{17})?$`

Campo obbligatorio: sì

Tags

Speciifica i tag che desideri applicare alla risorsa.

Tipo: matrice di oggetti TagListEntry

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK per Ruby V3

UntagResource

Rimuove i tag da una AWS risorsa.

Sintassi della richiesta

```
{
   "Keys": [ "string" ],
   "ResourceArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Keys

Specificate le chiavi nei tag che desiderate rimuovere.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:/-]+$`

Campo obbligatorio: sì

ResourceArn

Speciifica l'Amazon Resource Name (ARN) della risorsa da cui rimuovere i tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})(/execution/exec-[a-f0-9]{17})?$`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateAgent

Aggiorna il nome di un AWS DataSync agente.

Sintassi della richiesta

```
{
   "AgentArn": "string",
   "Name": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArn

L'Amazon Resource Name (ARN) dell'agente da aggiornare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: sì

Name

Il nome che desideri utilizzare per configurare l'agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationAzureBlob

Modifica le seguenti configurazioni della posizione di trasferimento di Microsoft Azure Blob Storage con cui stai usando. AWS DataSync

Per ulteriori informazioni, vedere Configurazione dei DataSync trasferimenti con Azure Blob Storage.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessTier

Speciifica il livello di accesso in cui desideri trasferire gli oggetti o i file. Ciò si applica solo quando si utilizza la posizione come destinazione di trasferimento. Per ulteriori informazioni, consulta Livelli di accesso.

Tipo: stringa

Valori validi: `HOT | COOL | ARCHIVE`

Campo obbligatorio: no

AgentArns

(Facoltativo) Specifica l'Amazon Resource Name (ARN) dell'agente che può connettersi DataSync al tuo contenitore Azure Blob Storage. Se stai configurando un trasferimento tra cloud senza agenti, non è necessario specificare un valore per questo parametro.

È possibile specificare più di un agente. Per ulteriori informazioni, consulta Utilizzo di più agenti per il trasferimento.

> **Note**
>
> Non è possibile aggiungere o rimuovere agenti da una posizione di archiviazione dopo averla creata inizialmente.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

AuthenticationType

Specifica il metodo di autenticazione DataSync usato per accedere al tuo archivio BLOB di Azure. DataSync può accedere all'archiviazione BLOB utilizzando una firma ad accesso condiviso (SAS).

Tipo: stringa

Valori validi: `SAS | NONE`

Campo obbligatorio: no

BlobType

Speciifica il tipo di blob che vuoi che siano i tuoi oggetti o file quando li trasferisci in Azure Blob Storage. Attualmente, supporta DataSync solo lo spostamento di dati in Azure Blob Storage

come block blob. Per altre informazioni sui tipi di blob, consulta la documentazione di Azure Blob Storage.

Tipo: stringa

Valori validi: `BLOCK`

Campo obbligatorio: no

CmkSecretConfig

Specifica le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione o un set di credenziali da DataSync utilizzare per accedere a una posizione di trasferimento specifica, e un segreto gestito dal cliente. AWS KMS key

Tipo: oggetto CmkSecretConfig

Campo obbligatorio: no

CustomSecretConfig

Speciifica le informazioni di configurazione per un segreto gestito dal cliente, ad esempio un token di autenticazione o un set di credenziali da DataSync utilizzare per accedere a una posizione di trasferimento specifica, e un segreto gestito dal cliente. AWS KMS key

Tipo: oggetto CustomSecretConfig

Campo obbligatorio: no

LocationArn

Speciifica l'ARN della posizione di trasferimento di Azure Blob Storage che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

SasConfiguration

Speciifica la configurazione SAS che consente di accedere DataSync al tuo Azure Blob Storage.

Tipo: oggetto AzureBlobSasConfiguration

Campo obbligatorio: no

Subdirectory

Specifica i segmenti di percorso se desideri limitare il trasferimento a una directory virtuale nel contenitore (ad esempio,). `/my/images`

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 1024.

Modello: `^[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}\p{C}]*$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationEfs

Modifica i seguenti parametri di configurazione della posizione di trasferimento Amazon EFS con AWS DataSync cui stai utilizzando.

Per ulteriori informazioni, consulta Configurazione dei DataSync trasferimenti con Amazon EFS.

Sintassi della richiesta

```
{
   "AccessPointArn": "string",
   "FileSystemAccessRoleArn": "string",
   "InTransitEncryption": "string",
   "LocationArn": "string",
   "Subdirectory": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessPointArn

Speciifica l'Amazon Resource Name (ARN) del punto di accesso utilizzato per DataSync montare il file system Amazon EFS.

Per ulteriori informazioni, consulta Accesso ai file system Amazon EFS con restrizioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `(^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$)|(^$)`

Campo obbligatorio: no

FileSystemAccessRoleArn

Specifica un ruolo AWS Identity and Access Management (IAM) che consente di accedere DataSync al file system Amazon EFS.

Per informazioni sulla creazione di questo ruolo, consulta Creazione di un ruolo DataSync IAM per l'accesso al file system Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `(^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$)|(^$)`

Campo obbligatorio: no

InTransitEncryption

Specifica se desideri DataSync utilizzare la crittografia Transport Layer Security (TLS) 1.2 quando trasferisce dati da o verso il tuo file system Amazon EFS.

Se specifichi un punto di accesso utilizzando `AccessPointArn` o un ruolo IAM utilizzando `FileSystemAccessRoleArn`, è necessario impostare questo parametro su `TLS1_2`.

Tipo: stringa

Valori validi: `NONE | TLS1_2`

Campo obbligatorio: no

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione di trasferimento Amazon EFS che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Subdirectory

Specifica un percorso di montaggio per il tuo file system Amazon EFS. È qui che DataSync legge o scrive i dati sul tuo file system (a seconda che si tratti di una posizione di origine o di destinazione).

Per impostazione predefinita, DataSync utilizza la directory principale (o il punto di accesso, se fornito utilizzando`AccessPointArn`). È inoltre possibile includere sottodirectory utilizzando barre (ad esempio,). `/path/to/folder`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationFsxLustre

Modifica i seguenti parametri di configurazione della posizione di trasferimento Amazon FSx for Lustre con cui stai utilizzando. AWS DataSync

Per ulteriori informazioni, consulta Configurazione dei DataSync trasferimenti con FSx for Lustre.

Sintassi della richiesta

```
{
   "LocationArn": "string",
   "Subdirectory": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) FSx della posizione di trasferimento for Lustre che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Subdirectory

Speciifica un percorso di montaggio per il file system FSx for Lustre. Il percorso può includere sottodirectory.

Quando la posizione viene utilizzata come fonte, DataSync legge i dati dal percorso di montaggio. Quando la posizione viene utilizzata come destinazione, DataSync scrive i dati nel percorso di

montaggio. Se non includete questo parametro, DataSync utilizza la directory principale del file system (/).

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationFsxOntap

Modifica i seguenti parametri di configurazione della posizione di trasferimento Amazon FSx for NetApp ONTAP con cui stai utilizzando. AWS DataSync

Per ulteriori informazioni, consulta Configurazione dei DataSync trasferimenti con FSx for ONTAP.

Sintassi della richiesta

```
{
   "LocationArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "Subdirectory": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) FSx della posizione di trasferimento for ONTAP che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Protocol

Speciifica il protocollo di trasferimento dati DataSync utilizzato per accedere al tuo FSx file system Amazon.

Tipo: oggetto FsxUpdateProtocol

Campo obbligatorio: no

Subdirectory

Speciifica il percorso della condivisione di file nella macchina virtuale di archiviazione (SVM) da cui desideri trasferire i dati.

Puoi specificare un percorso di giunzione (detto anche punto di montaggio), un percorso qtree (per condivisioni di file NFS) o un nome condivisione (per condivisioni di file SMB). Ad esempio, il percorso di montaggio potrebbe essere `/vol1`, `/vol1/tree1`, o `/share1`.

> **Note**
>
> Non specificare un percorso di giunzione nel volume radice dell'SVM. Per ulteriori informazioni, consulta Managing FSx for ONTAP Storage Virtual Machines nella Amazon FSx for NetApp ONTAP User Guide.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationFsxOpenZfs

Modifica i seguenti parametri di configurazione della posizione di trasferimento Amazon FSx for OpenZFS con cui stai utilizzando. AWS DataSync

Per maggiori informazioni, consulta Configurazione dei DataSync trasferimenti con per OpenZFS. FSx

> **Note**
>
> I parametri di richiesta relativi a SMB non sono supportati dall'operazione. `UpdateLocationFsxOpenZfs`

Sintassi della richiesta

```
{
   "LocationArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "Subdirectory": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) FSx della posizione di trasferimento per OpenZFS che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Protocol

Speciifica il protocollo di trasferimento dati AWS DataSync utilizzato per accedere al tuo FSx file system Amazon.

Tipo: oggetto FsxProtocol

Campo obbligatorio: no

Subdirectory

Speciifica una sottodirectory nel percorso della posizione che deve iniziare con. `/fsx` DataSync utilizza questa sottodirectory per leggere o scrivere dati (a seconda che il file system sia una posizione di origine o di destinazione).

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationFsxWindows

Modifica i seguenti parametri di configurazione della posizione di trasferimento di Amazon FSx for Windows File Server con AWS DataSync cui stai utilizzando.

Per ulteriori informazioni, consulta Configurazione dei DataSync trasferimenti con FSx per Windows File Server.

Sintassi della richiesta

```
{
   "Domain": "string",
   "LocationArn": "string",
   "Password": "string",
   "Subdirectory": "string",
   "User": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Domain

Speciifica il nome del dominio Windows a cui appartiene il file system FSx per Windows File Server.

Se nell'ambiente sono presenti più domini Active Directory, la configurazione di questo parametro assicura la DataSync connessione al file system corretto.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^([A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252})?$`

Campo obbligatorio: no

LocationArn

Speciifica l'ARN FSx della posizione di trasferimento per Windows File Server che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

Password

Speciifica la password dell'utente con le autorizzazioni per montare e accedere a file, cartelle e metadati dei file nel file system FSx per Windows File Server.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^.{0,104}$`

Campo obbligatorio: no

Subdirectory

Specificate un percorso di montaggio per il file system utilizzando barre. DataSync utilizza questa sottodirectory per leggere o scrivere dati (a seconda che il file system sia una posizione di origine o di destinazione).

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

User

Speciifica l'utente con le autorizzazioni per montare e accedere a file, cartelle e metadati dei file nel file system FSx per Windows File Server.

Per informazioni sulla scelta di un utente con il giusto livello di accesso per il trasferimento, consulta le autorizzazioni richieste FSx per le posizioni dei file server di Windows.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationHdfs

Modifica i seguenti parametri di configurazione della posizione di trasferimento Hadoop Distributed File System (HDFS) con cui stai utilizzando. AWS DataSync

Per ulteriori informazioni, consulta Configurazione dei DataSync trasferimenti con un cluster HDFS.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArns

Gli Amazon Resource Names (ARNs) degli DataSync agenti che possono connettersi al tuo cluster HDFS.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

AuthenticationType

Il tipo di autenticazione utilizzato per determinare l'identità dell'utente.

Tipo: stringa

Valori validi: `SIMPLE | KERBEROS`

Campo obbligatorio: no

BlockSize

La dimensione dei blocchi di dati da scrivere nel cluster HDFS.

Tipo: integer

Intervallo valido: valore minimo di 1048576. Valore massimo di 1073741824.

Campo obbligatorio: no

KerberosKeytab

La tabella delle chiavi Kerberos (keytab) che contiene le mappature tra il principali Kerberos definiti e le chiavi crittografate. È possibile caricare il keytab da un file fornendo l'indirizzo del file.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 65536.

Campo obbligatorio: no

KerberosKrb5Conf

Il file `krb5.conf` che contiene le informazioni di configurazione di Kerberos. È possibile caricare il `krb5.conf` file fornendo l'indirizzo del file. Se stai usando AWS CLI, esegue la codifica base64 per te. Altrimenti, fornisci il testo con codifica base64.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 131072.

Campo obbligatorio: no

KerberosPrincipal

Il principale Kerberos con accesso ai file e alle cartelle sul cluster HDFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^.+$`

Campo obbligatorio: no

KmsKeyProviderUri

L'URI del Key Management Server (KMS) del cluster HDFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `^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$`

Campo obbligatorio: no

LocationArn

L'Amazon Resource Name (ARN) della posizione del cluster HDFS di origine.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

NameNodes

Il NameNode che gestisce lo spazio dei nomi HDFS. NameNode Esegue operazioni come l'apertura, la chiusura e la ridenominazione di file e directory. NameNode Contiene le informazioni per mappare blocchi di dati su. DataNodes È possibile utilizzarne solo uno NameNode.

Tipo: matrice di oggetti HdfsNameNode

Membri dell'array: numero minimo di 1 elemento.

Campo obbligatorio: no

QopConfiguration

La configurazione QOP (Quality of Protection) specifica le impostazioni di privacy per le chiamate di procedura remota (RPC, Remote Procedure Call) e per il trasferimento dati configurate nel cluster del file system distribuito Hadoop (HDFS).

Tipo: oggetto QopConfiguration

Campo obbligatorio: no

ReplicationFactor

Il numero DataNodes su cui replicare i dati durante la scrittura sul cluster HDFS.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 512.

Campo obbligatorio: no

SimpleUser

Il nome utente utilizzato per identificare il client sul sistema operativo host.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

Campo obbligatorio: no

Subdirectory

Una sottodirectory nel cluster HDFS. Questa sottodirectory viene utilizzata per leggere i dati da o scrivere i dati sul cluster HDFS.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationNfs

Modifica i seguenti parametri di configurazione della posizione di trasferimento Network File System (NFS) con cui si sta utilizzando. AWS DataSync

Per ulteriori informazioni, consulta Configurazione dei trasferimenti con un file server NFS.

Sintassi della richiesta

```
{
   "LocationArn": "string",
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
   },
   "ServerHostname": "string",
   "Subdirectory": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Specifica l'Amazon Resource Name (ARN) della posizione di trasferimento NFS che desideri aggiornare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

MountOptions

Specifica come DataSync accedere a una posizione utilizzando il protocollo NFS.

Tipo: oggetto NfsMountOptions

Campo obbligatorio: no

OnPremConfig

Gli AWS DataSync agenti che possono connettersi al file server Network File System (NFS).

Tipo: oggetto OnPremConfig

Campo obbligatorio: no

ServerHostname

Speciifica il nome DNS o l'indirizzo IP (IPv4 o IPv6) del file server NFS a cui si connette DataSync l'agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Campo obbligatorio: no

Subdirectory

Specificate il percorso di esportazione nel file server NFS che desiderate montare. DataSync

Questo percorso (o una sottodirectory del percorso) è il luogo in cui vengono DataSync trasferiti i dati da o verso. Per informazioni sulla configurazione di un'esportazione per DataSync, consultate Accesso ai file server NFS.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]+$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationObjectStorage

Modifica i seguenti parametri di configurazione della posizione di trasferimento dell'archiviazione degli oggetti con AWS DataSync cui si sta utilizzando.

Per ulteriori informazioni, vedere Configurazione dei DataSync trasferimenti con un sistema di storage di oggetti.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessKey

Specifica la chiave di accesso (ad esempio, un nome utente) se sono necessarie credenziali per l'autenticazione con il server di storage di oggetti.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `^.*$`

Campo obbligatorio: no

AgentArns

(Facoltativo) Speciifica gli Amazon Resource Names (ARNs) degli DataSync agenti che possono connettersi al tuo sistema di storage di oggetti. Se stai configurando un trasferimento tra cloud senza agenti, non è necessario specificare un valore per questo parametro.

> **Note**
>
> Non è possibile aggiungere o rimuovere agenti da una posizione di archiviazione dopo averla creata inizialmente.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

CmkSecretConfig

Specifica le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione o un set di credenziali da DataSync utilizzare per accedere a una posizione di trasferimento specifica, e un segreto gestito dal cliente. AWS KMS key

Tipo: oggetto CmkSecretConfig

Campo obbligatorio: no

CustomSecretConfig

Speciifica le informazioni di configurazione per un segreto gestito dal cliente, ad esempio un token di autenticazione o un set di credenziali da DataSync utilizzare per accedere a una posizione di trasferimento specifica, e un segreto gestito dal cliente. AWS KMS key

Tipo: oggetto CustomSecretConfig

Campo obbligatorio: no

LocationArn

Specifica l'ARN della posizione del sistema di storage degli oggetti che si sta aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

SecretKey

Specifica la chiave segreta (ad esempio, una password) se sono necessarie credenziali per l'autenticazione con il server di storage di oggetti.

> **Note**
>
> Se fornisci un segreto utilizzando`SecretKey`, ma non fornisci dettagli di configurazione segreti utilizzando `CmkSecretConfig` o`CustomSecretConfig`, DataSync archivia il token utilizzando il segreto di Secrets Manager del tuo AWS account.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `^.*$`

Campo obbligatorio: no

ServerCertificate

Speciifica una catena di certificati DataSync per l'autenticazione con il sistema di archiviazione degli oggetti se il sistema utilizza un'autorità di certificazione (CA) privata o autofirmata. È necessario specificare un singolo `.pem` file con una catena di certificati completa (ad esempio,). `file:///home/user/.ssh/object_storage_certificates.pem`

La catena di certificati potrebbe includere:

- Il certificato del sistema di archiviazione degli oggetti
- Tutti i certificati intermedi (se presenti)
- Il certificato principale della CA firmataria

È possibile concatenare i certificati in un `.pem` file (che può contenere fino a 32768 byte prima della codifica in base64). Il `cat` comando di esempio seguente crea un file che include tre certificati: `object_storage_certificates.pem`

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

Per utilizzare questo parametro, `ServerProtocol` configurare su`HTTPS`.

L'aggiornamento di questo parametro non interferisce con le attività in corso.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 32768.

Campo obbligatorio: no

ServerHostname

Speciifica il nome di dominio o l'indirizzo IP (IPv4 o IPv6) del server di archiviazione degli oggetti a cui si connette DataSync l'agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Campo obbligatorio: no

ServerPort

Specifica la porta su cui il server di storage di oggetti accetta il traffico di rete in ingresso (ad esempio la porta 443).

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 65536.

Campo obbligatorio: no

ServerProtocol

Specifica il protocollo utilizzato dal server di storage di oggetti per comunicare.

Tipo: stringa

Valori validi: `HTTPS | HTTP`

Campo obbligatorio: no

Subdirectory

Specifica il prefisso dell'oggetto per il server di storage di oggetti. Se si tratta di una posizione di origine, copia DataSync solo gli oggetti con questo prefisso. Se si tratta di una posizione di destinazione, DataSync scrive tutti gli oggetti con questo prefisso.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationS3

Modifica i seguenti parametri di configurazione della posizione di trasferimento Amazon S3 con cui stai utilizzando. AWS DataSync

> **Important**
>
> Prima di iniziare, assicurati di leggere i seguenti argomenti:
>
> - Considerazioni sulla classe di storage con le sedi Amazon S3
> - Valutazione dei costi delle richieste S3 durante l'utilizzo DataSync

Sintassi della richiesta

```
{
   "LocationArn": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
   "S3StorageClass": "string",
   "Subdirectory": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

LocationArn

Speciifica l'Amazon Resource Name (ARN) della posizione di trasferimento Amazon S3 che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

S3Config

Speciifica l'Amazon Resource Name (ARN) AWS Identity and Access Management del ruolo DataSync (IAM) utilizzato per accedere al bucket S3.

Per ulteriori informazioni, consulta Fornire l' DataSync accesso ai bucket S3.

Tipo: oggetto S3Config

Campo obbligatorio: no

S3StorageClass

Speciifica la classe di storage che desideri che i tuoi oggetti utilizzino quando Amazon S3 è una destinazione di trasferimento.

Per i bucket in Regioni AWS, la classe di storage predefinita è. `STANDARD` Per i bucket attivi AWS Outposts, la classe di archiviazione ha come impostazione predefinita. `OUTPOSTS`

Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con i trasferimenti Amazon S3.

Tipo: stringa

Valori validi: `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

Campo obbligatorio: no

Subdirectory

Speciifica un prefisso nel bucket S3 da cui eseguire la DataSync lettura o la scrittura (a seconda che il bucket sia una posizione di origine o di destinazione).

> **Note**
>
> DataSync non può trasferire oggetti con un prefisso che inizia con una barra () `/` o include o pattern. `//` `/./` `/../` Per esempio:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`

- `photos/../2006/March`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateLocationSmb

Modifica i seguenti parametri di configurazione della posizione di trasferimento Server Message Block (SMB) con cui stai utilizzando. AWS DataSync

Per ulteriori informazioni, consulta Configurazione dei DataSync trasferimenti con un file server SMB.

Sintassi della richiesta

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosKeytab": blob,
   "KerberosKrb5Conf": blob,
   "KerberosPrincipal": "string",
   "LocationArn": "string",
   "MountOptions": {
      "Version": "string"
   },
   "Password": "string",
   "ServerHostname": "string",
   "Subdirectory": "string",
   "User": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgentArns

Speciifica l' DataSync agente (o gli agenti) che possono connettersi al file server SMB. Specifichi un agente utilizzando il relativo Amazon Resource Name (ARN).

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

AuthenticationType

Speciifica il protocollo di autenticazione DataSync utilizzato per connettersi al file server SMB. DataSync supporta `NTLM` (impostazione predefinita) e `KERBEROS` autenticazione.

Per ulteriori informazioni, vedere Fornire DataSync l'accesso ai file server SMB.

Tipo: stringa

Valori validi: `NTLM | KERBEROS`

Campo obbligatorio: no

DnsIpAddresses

Speciifica gli indirizzi IP (IPv4 o IPv6) per i server DNS a cui appartiene il file server SMB. Questo parametro si applica solo se `AuthenticationType` è impostato su. `KERBEROS`

Se nell'ambiente sono presenti più domini, la configurazione di questo parametro assicura la DataSync connessione al file server SMB corretto.

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 2 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 7. Lunghezza massima di 39.

Modello: `\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`

Campo obbligatorio: no

Domain

Specifica il nome dominio di Windows a cui appartiene il server di file SMB. Questo parametro si applica solo se `AuthenticationType` è impostato su`NTLM`.

Se nell'ambiente sono presenti più domini, la configurazione di questo parametro assicura la DataSync connessione al file server corretto.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Campo obbligatorio: no

KerberosKeytab

Speciifica il file della tabella delle chiavi Kerberos (keytab), che include le mappature tra la chiave principale Kerberos e la chiave di crittografia.

Per evitare errori di esecuzione delle attività, assicurati che il principale Kerberos utilizzato per creare il file keytab corrisponda esattamente a quello specificato. `KerberosPrincipal`

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 65536.

Campo obbligatorio: no

KerberosKrb5Conf

Specifica un file di configurazione Kerberos (`krb5.conf`) che definisce la configurazione del realm Kerberos.

Il file deve essere codificato in base 64. Se stai usando il AWS CLI, la codifica è pronta per te.

Tipo: oggetto dati binari con codifica Base64

Vincoli di lunghezza: lunghezza massima di 131072.

Campo obbligatorio: no

KerberosPrincipal

Speciifica un principale Kerberos, che è un'identità nell'area di autenticazione Kerberos autorizzata ad accedere a file, cartelle e metadati dei file nel file server SMB.

Potrebbe essere simile `HOST/kerberosuser@MYDOMAIN.ORG` a un principale Kerberos.

I nomi principali distinguono tra maiuscole e minuscole. L'esecuzione dell' DataSync attività avrà esito negativo se il principale specificato per questo parametro non corrisponde esattamente al principale utilizzato per creare il file keytab.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^.+$`

Campo obbligatorio: no

LocationArn

Specificare l'ARN della posizione SMB che si desidera aggiornare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: sì

MountOptions

Speciifica la versione del protocollo Server Message Block (SMB) AWS DataSync utilizzata per accedere a un file server SMB.

Tipo: oggetto SmbMountOptions

Campo obbligatorio: no

Password

Speciifica la password dell'utente che può montare il file server SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento. Questo parametro si applica solo se `AuthenticationType` è impostato su. `NTLM`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^.{0,104}$`

Campo obbligatorio: no

ServerHostname

Speciifica il nome di dominio o l'indirizzo IP (IPv4 o IPv6) del file server SMB a cui l'agente si connette DataSync .

> **Note**
>
> Se utilizzi l'autenticazione Kerberos, devi specificare un nome di dominio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 255.

Modello: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Campo obbligatorio: no

Subdirectory

Speciifica il nome della condivisione esportata dal file server SMB in cui leggerà o DataSync scriverà i dati. È possibile includere una sottodirectory nel percorso di condivisione (ad esempio,). `/path/to/subdirectory` Assicurati che anche altri client SMB della tua rete possano montare questo percorso.

Per copiare tutti i dati nella sottodirectory specificata, DataSync deve essere in grado di montare la condivisione SMB e accedere a tutti i relativi dati. Per ulteriori informazioni, vedere Fornire DataSync l'accesso ai file server SMB.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Campo obbligatorio: no

User

Speciifica il nome utente che può montare il file server SMB e dispone dell'autorizzazione per accedere ai file e alle cartelle coinvolti nel trasferimento. Questo parametro si applica solo se `AuthenticationType` è impostato su. `NTLM`

Per informazioni sulla scelta di un utente con il giusto livello di accesso per il trasferimento, consulta Fornire DataSync l'accesso ai file server SMB.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateTask

Aggiorna la configurazione di un'attività, che definisce dove e come vengono AWS DataSync trasferiti i dati.

Sintassi della richiesta

```
{
   "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"
   }
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

CloudWatchLogGroupArn

Speciifica l'Amazon Resource Name (ARN) di un gruppo di log CloudWatch Amazon per il monitoraggio dell'attività.

Per le attività in modalità avanzata, devi utilizzare `/aws/datasync` come nome del gruppo di log. Per esempio:

`arn:aws:logs:us-east-1:111222333444:log-group:/aws/datasync:*`

Per ulteriori informazioni, vedere Monitoraggio dei trasferimenti di dati con CloudWatch i registri.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 562.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

Campo obbligatorio: no

Excludes

Speciifica i filtri di esclusione che definiscono i file, gli oggetti e le cartelle nella posizione di origine che non si desidera trasferire. DataSync Per ulteriori informazioni ed esempi, consulta Specificare DataSync i trasferimenti utilizzando i filtri.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

Includes

I filtri di inclusione specificano i file, gli oggetti e le cartelle che si desidera DataSync trasferire nella posizione di origine. Per ulteriori informazioni ed esempi, vedere Specificazione dei DataSync trasferimenti utilizzando i filtri.

Tipo: matrice di oggetti FilterRule

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

ManifestConfig

Configura un manifesto, che è un elenco di file o oggetti che si desidera DataSync trasferire. Per ulteriori informazioni ed esempi di configurazione, vedere Specificazione degli elementi da DataSync trasferire utilizzando un manifesto.

Quando si utilizza questo parametro, l'identità del chiamante (il ruolo IAM DataSync con cui si utilizza) deve disporre dell'`iam:PassRole`autorizzazione. La AWSDataSyncFullAccesspolitica include questa autorizzazione.

Per rimuovere una configurazione del manifesto, specificate questo parametro come vuoto.

Tipo: oggetto ManifestConfig

Campo obbligatorio: no

Name

Specificate il nome dell'attività.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

Options

Indica come è configurata l'attività di trasferimento. Queste opzioni includono la modalità DataSync di gestione dei file, degli oggetti e dei metadati associati durante il trasferimento. Puoi anche specificare come verificare l'integrità dei dati, impostare limiti di larghezza di banda per l'attività, tra le altre opzioni.

Ogni opzione ha un valore predefinito. A meno che non sia necessario, non è necessario configurare alcuna opzione prima di chiamare StartTaskExecution.

È inoltre possibile sovrascrivere le opzioni dell'attività per ogni esecuzione di attività. Ad esempio, potresti voler modificare il valore `LogLevel` per una singola esecuzione.

Tipo: oggetto Options

Campo obbligatorio: no

Schedule

Specificate una pianificazione in base alla quale desiderate che l'attività venga eseguita. Per ulteriori informazioni, vedere Pianificazione delle attività.

Tipo: oggetto TaskSchedule

Campo obbligatorio: no

TaskArn

Specificare l'ARN dell'attività che si desidera aggiornare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Campo obbligatorio: sì

TaskReportConfig

Specifica come si desidera configurare un rapporto sulle attività, che fornisce informazioni dettagliate sul trasferimento. DataSync Per ulteriori informazioni, consulta Monitoraggio dei DataSync trasferimenti con report sulle attività.

Quando utilizzi questo parametro, l'identità del chiamante (il ruolo IAM DataSync con cui stai utilizzando) deve disporre dell'`iam:PassRole`autorizzazione. La AWSDataSyncFullAccesspolitica include questa autorizzazione.

Per rimuovere la configurazione di un report di attività, specificate questo parametro come vuoto.

Tipo: oggetto TaskReportConfig

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel AWS DataSync servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateTaskExecution

Aggiorna la configurazione dell'esecuzione di un' AWS DataSync attività in esecuzione.

> **Note**
>
> Attualmente, l'unica opzione `Option` che è possibile modificare `UpdateTaskExecution` è `BytesPerSecond` , che limita la larghezza di banda per l'esecuzione di un'attività in esecuzione o in coda.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Options

Indica come è configurata l'operazione di trasferimento. Queste opzioni includono la modalità DataSync di gestione dei file, degli oggetti e dei metadati associati durante il trasferimento. Puoi anche specificare come verificare l'integrità dei dati, impostare limiti di larghezza di banda per l'attività, tra le altre opzioni.

Ogni opzione ha un valore predefinito. A meno che non sia necessario, non è necessario configurare alcuna opzione prima di chiamare StartTaskExecution.

È inoltre possibile sovrascrivere le opzioni dell'attività per ogni esecuzione di attività. Ad esempio, potresti voler modificare il valore `LogLevel` per una singola esecuzione.

Tipo: oggetto Options

Campo obbligatorio: sì

TaskExecutionArn

Speciifica l'Amazon Resource Name (ARN) dell'esecuzione dell'attività che stai aggiornando.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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}$`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalException

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS DataSync

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

Tipi di dati

Sono supportati i tipi di dati seguenti:

- 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
- TaskExecutionListEntry
- TaskExecutionResultDetail
- TaskFilter
- TaskListEntry

- TaskReportConfig
- TaskSchedule
- TaskScheduleDetails

AgentListEntry

Rappresenta una singola voce in un elenco (o matrice) di AWS DataSync agenti quando si chiama l'ListAgentsoperazione.

Indice

AgentArn

L'Amazon Resource Name (ARN) di un DataSync agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: no

Name

Il nome di un agente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

Platform

I dettagli relativi alla piattaforma sull'agente, ad esempio il numero di versione.

Tipo: oggetto Platform

Campo obbligatorio: no

Status

Lo stato di un agente.

- Se lo stato è`ONLINE`, l'agente è configurato correttamente e pronto per l'uso.

- Se lo stato è`OFFLINE`, l'agente non è in contatto con l'agente DataSync da cinque minuti o più. Questo può succedere per diversi motivi. Per ulteriori informazioni, vedi Cosa devo fare se il mio agente è offline?

Tipo: stringa

Valori validi: `ONLINE | OFFLINE`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

AzureBlobSasConfiguration

La configurazione SAS (Shared Access Signature) che consente di accedere AWS DataSync al tuo Microsoft Azure Blob Storage.

Per ulteriori informazioni, vedi Token SAS per accedere al tuo Azure Blob Storage.

Indice

Token

Specifica un token SAS che fornisce le autorizzazioni per accedere al tuo Azure Blob Storage.

Il token fa parte della stringa URI SAS che segue l'URI della risorsa di archiviazione e un punto interrogativo. Un token ha un aspetto simile al seguente:

```
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
```

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `^.+$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CmkSecretConfig

Specifica le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione o una chiave segreta da DataSync utilizzare per accedere a una posizione di archiviazione specifica, con un segreto gestito dal cliente. AWS KMS key

> **Note**
>
> È possibile utilizzare una delle due opzioni `CmkSecretConfig` o fornire le credenziali `CustomSecretConfig` per una richiesta. `CreateLocation` Non fornire entrambi i parametri per la stessa richiesta.

Indice

KmsKeyArn

Speciifica l'ARN per il codice gestito dal AWS KMS key cliente utilizzato per DataSync crittografare il segreto gestito DataSync per. `SecretArn` DataSync fornisce questa chiave a. AWS Secrets Manager

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):kms:[a-z\-0-9]+:[0-9]{12}:key/.*|)$`

Campo obbligatorio: no

SecretArn

Speciifica l'ARN per DataSync il AWS Secrets Manager -managed secret utilizzato per accedere a una posizione di archiviazione specifica. Questa proprietà è generata da DataSync ed è di sola lettura. DataSync crittografa questo segreto con la chiave KMS specificata dall'utente. `KmsKeyArn`

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CustomSecretConfig

Specifica le informazioni di configurazione per un segreto di Secrets Manager gestito dal cliente in cui un token di autenticazione della posizione di archiviazione o una chiave segreta è archiviato in testo semplice. Questa configurazione include l'ARN segreto e l'ARN per un ruolo IAM che fornisce l'accesso al segreto.

> **Note**
>
> È possibile utilizzare uno `CmkSecretConfig` o l'altro `CustomSecretConfig` per fornire le credenziali per una richiesta. `CreateLocation` Non fornire entrambi i parametri per la stessa richiesta.

Indice

SecretAccessRoleArn

Speciifica l'ARN per AWS Identity and Access Management il ruolo DataSync utilizzato per accedere al segreto specificato per. `SecretArn`

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/[a-zA-Z0-9+=,.@_-]+|)$`

Campo obbligatorio: no

SecretArn

Speciifica l'ARN per AWS Secrets Manager un segreto.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Ec2Config

La sottorete e i gruppi di sicurezza AWS DataSync utilizzati per connettersi a uno degli obiettivi di montaggio del file system Amazon EFS.

Indice

SecurityGroupArns

Speciifica gli Amazon Resource Names (ARNs) dei gruppi di sicurezza associati alla destinazione di montaggio di un file system Amazon EFS.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Campo obbligatorio: sì

SubnetArn

Speciifica l'ARN di una sottorete in DataSync cui crea le interfacce di rete per la gestione del traffico durante il trasferimento.

La sottorete deve trovarsi:

- Nello stesso cloud privato virtuale (VPC) del file system Amazon EFS.
- Nella stessa zona di disponibilità di almeno una destinazione di montaggio per il file system Amazon EFS.

> **Note**
>
> Non è necessario specificare una sottorete che presenti una destinazione di montaggio del file system.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/.*$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

FilterRule

Specifica quali file, cartelle e oggetti includere o escludere durante il trasferimento dei file dall'origine alla destinazione.

Indice

FilterType

Il tipo di regola di filtro da applicare. AWS DataSync supporta solo il tipo di regola SIMPLE_PATTERN.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^[A-Z0-9_]+$`

Valori validi: `SIMPLE_PATTERN`

Campo obbligatorio: no

Value

Una singola stringa di filtro costituita dai modelli da includere o escludere. I modelli sono delimitati da "|" (cioè una barra verticale), ad esempio: `/folder1|/folder2`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 102400.

Modello: `^[^\x00]+$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++

- AWS SDK per Java V2
- AWS SDK per Ruby V3

FsxProtocol

Speciifica il protocollo di trasferimento dati AWS DataSync utilizzato per accedere al tuo FSx file system Amazon.

Indice

NFS

Speciifica la configurazione del protocollo Network File System (NFS) da DataSync utilizzare FSx per accedere al file system per OpenZFS o FSx alla macchina virtuale di archiviazione (SVM) del file system ONTAP.

Tipo: oggetto FsxProtocolNfs

Campo obbligatorio: no

SMB

Specifica la configurazione del protocollo Server Message Block (SMB) da DataSync utilizzare per accedere alla SVM del file system for ONTAP. FSx

Tipo: oggetto FsxProtocolSmb

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consultate quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

FsxProtocolNfs

Specifica la configurazione del protocollo Network File System (NFS) da DataSync utilizzare FSx per accedere al file system per OpenZFS o alla macchina virtuale di archiviazione (FSx SVM) del file system ONTAP.

Indice

MountOptions

Speciifica come accedere a una posizione utilizzando il DataSync protocollo NFS.

Tipo: oggetto NfsMountOptions

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

FsxProtocolSmb

Speciifica la configurazione del protocollo Server Message Block (SMB) da AWS DataSync utilizzare per accedere alla macchina virtuale di archiviazione (SVM) del file system Amazon FSx for NetApp ONTAP. Per ulteriori informazioni, consulta Fornire DataSync l'accesso ai file system ONTAP FSx .

Indice

Password

Specifica la password di un utente che dispone dell'autorizzazione per accedere a SVM.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^.{0,104}$`

Campo obbligatorio: sì

User

Speciifica un utente in grado di montare e accedere a file, cartelle e metadati nella SVM.

Per informazioni sulla scelta di un utente con il giusto livello di accesso per il trasferimento, consulta Uso del protocollo SMB.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Campo obbligatorio: sì

Domain

Speciifica il nome del dominio Windows a cui appartiene la macchina virtuale di archiviazione (SVM).

Se nel tuo ambiente sono presenti più domini, la configurazione di questa impostazione assicura che DataSync si connetta alla SVM corretta.

Se nel tuo ambiente sono presenti più domini Active Directory, la configurazione di questo parametro assicura che DataSync si connetta alla SVM corretta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Campo obbligatorio: no

MountOptions

Speciifica la versione del protocollo Server Message Block (SMB) da AWS DataSync utilizzare per accedere a un file server SMB.

Tipo: oggetto SmbMountOptions

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

FsxUpdateProtocol

Speciifica il protocollo di trasferimento dati AWS DataSync utilizzato per accedere al tuo FSx file system Amazon.

> **Note**
>
> Non puoi aggiornare la configurazione del protocollo Network File System (NFS) FSx per le sedi ONTAP. DataSync attualmente supporta solo la versione 3 di NFS con questo tipo di posizione.

Indice

NFS

Speciifica la configurazione del protocollo Network File System (NFS) da DataSync utilizzare FSx per accedere al file system per OpenZFS o FSx alla macchina virtuale di archiviazione (SVM) del file system ONTAP.

Tipo: oggetto FsxProtocolNfs

Campo obbligatorio: no

SMB

Speciifica la configurazione del protocollo Server Message Block (SMB) da DataSync utilizzare per accedere alla macchina virtuale di archiviazione (SVM) del file system FSx for ONTAP.

Tipo: oggetto FsxUpdateProtocolSmb

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2

- AWS SDK per Ruby V3

FsxUpdateProtocolSmb

Speciifica la configurazione del protocollo Server Message Block (SMB) da AWS DataSync utilizzare per accedere alla macchina virtuale di archiviazione (SVM) del file system Amazon FSx for NetApp ONTAP. Per ulteriori informazioni, consulta Fornire DataSync l'accesso ai file system ONTAP FSx .

Indice

Domain

Speciifica il nome del dominio Windows a cui appartiene la macchina virtuale di archiviazione (SVM).

Se nel tuo ambiente sono presenti più domini Active Directory, la configurazione di questo parametro assicura che DataSync si connetta alla SVM corretta.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 253.

Modello: `^([A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252})?$`

Campo obbligatorio: no

MountOptions

Speciifica la versione del protocollo Server Message Block (SMB) da AWS DataSync utilizzare per accedere a un file server SMB.

Tipo: oggetto SmbMountOptions

Campo obbligatorio: no

Password

Specifica la password di un utente che dispone dell'autorizzazione per accedere a SVM.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^.{0,104}$`

Campo obbligatorio: no

User

Speciifica un utente in grado di montare e accedere a file, cartelle e metadati nella SVM.

Per informazioni sulla scelta di un utente con il giusto livello di accesso per il trasferimento, consulta Uso del protocollo SMB.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 104.

Modello: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

HdfsNameNode

Il NameNode sistema Hadoop Distributed File System (HDFS). NameNode Gestisce lo spazio dei nomi del file system. NameNode Esegue operazioni come l'apertura, la chiusura e la ridenominazione di file e directory. NameNode Contiene le informazioni per mappare blocchi di dati su. DataNodes

Indice

Hostname

Il nome host di NameNode nel cluster HDFS. Questo valore è l'indirizzo IP o il nome DNS (Domain Name Service) di. NameNode Un agente installato in locale utilizza questo nome host per comunicare con loro NameNode nella rete.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9])$`

Campo obbligatorio: sì

Port

La porta che NameNode utilizza per ascoltare le richieste dei client.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 65536.

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

LocationFilter

Restringi l'elenco delle risorse restituite da`ListLocations`. Ad esempio, per visualizzare tutte le tue sedi Amazon S3, crea un filtro utilizzando `"Name": "LocationType""Operator": "Equals"`, e. `"Values": "S3"`

Per ulteriori informazioni, consulta Filtraggio delle risorse.

Indice

Name

Il nome del filtro utilizzato. Ogni chiamata API supporta un elenco di filtri disponibili (ad esempio, `LocationType` per`ListLocations`).

Tipo: stringa

Valori validi: `LocationUri | LocationType | CreationTime`

Campo obbligatorio: sì

Operator

L'operatore utilizzato per confrontare i valori dei filtri (ad esempio, `Equals` o`Contains`).

Tipo: stringa

Valori validi: `Equals | NotEquals | In | LessThanOrEqual | LessThan | GreaterThanOrEqual | GreaterThan | Contains | NotContains | BeginsWith`

Campo obbligatorio: sì

Values

I valori in base ai quali si desidera filtrare. Ad esempio, potresti voler visualizzare solo le sedi Amazon S3.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `^[0-9a-zA-Z_\ \-\:\*\.\\/\?-]*$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

LocationListEntry

Rappresenta una singola voce in un elenco di posizioni. `LocationListEntry`restituisce un array che contiene un elenco di posizioni quando viene chiamata l'ListLocationsoperazione.

Indice

LocationArn

L'Amazon Resource Name (ARN) della posizione. Per Network File System (NFS) o Amazon EFS, la posizione è il percorso di esportazione. Per Amazon S3, la posizione è il percorso del prefisso che desideri montare e utilizzare come radice della posizione.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Campo obbligatorio: no

LocationUri

Rappresenta un elenco URIs di una posizione. `LocationUri`restituisce un array che contiene un elenco di posizioni quando viene chiamata l'ListLocationsoperazione.

Formato:`TYPE://GLOBAL_ID/SUBDIR`.

TYPE indica il tipo di posizione (ad esempio, `nfs` `os3`).

GLOBAL_ID è l'identificatore univoco globale della risorsa che supporta la posizione. Un esempio per EFS è`us-east-2.fs-abcd1234`. Un esempio per Amazon S3 è il nome del bucket, ad esempio. `myBucket` Un esempio di NFS è un IPv6 indirizzo IPv4 or o un nome host valido conforme al DNS.

SUBDIR è un percorso di file system valido, delimitato da barre, così come la convenzione*nix. Per NFS e Amazon EFS, è il percorso di esportazione per montare la posizione. Per Amazon S3, è il percorso del prefisso su cui monti e che consideri come radice della posizione.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4360.

Modello: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ManagedSecretConfig

Specifica le informazioni di configurazione per un segreto DataSync gestito, ad esempio un token di autenticazione o un set di credenziali da DataSync utilizzare per accedere a una posizione di trasferimento specifica. DataSync utilizza la chiave KMS AWS gestita di default per crittografare questo segreto. AWS Secrets Manager

Indice

SecretArn

Speciifica l'ARN per AWS Secrets Manager un segreto.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ManifestConfig

Configura un manifesto, che è un elenco di file o oggetti che si desidera AWS DataSync trasferire. Per ulteriori informazioni ed esempi di configurazione, vedere Specificazione degli elementi da DataSync trasferire utilizzando un manifesto.

Indice

Action

Speciifica per cosa DataSync viene utilizzato il manifesto.

Tipo: stringa

Valori validi: `TRANSFER`

Campo obbligatorio: no

Format

Speciifica il formato di file del manifesto. Per ulteriori informazioni, vedere Creazione di un manifesto.

Tipo: stringa

Valori validi: `CSV`

Campo obbligatorio: no

Source

Specificate il manifesto che desiderate DataSync utilizzare e dove è ospitato.

> **Note**
>
> È necessario specificare questo parametro se si sta configurando un nuovo manifesto a partire dal 7 febbraio 2024.
> In caso contrario, riceverai un codice di stato 400 e un `ValidationException` errore che indica che ti manca il ruolo IAM per accedere DataSync al bucket S3 in cui stai ospitando il tuo manifest. Per ulteriori informazioni, consulta Fornire DataSync l'accesso al tuo manifest.

Tipo: oggetto SourceManifestConfig

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

NfsMountOptions

Specifica come DataSync accedere a una posizione utilizzando il protocollo NFS.

Indice

Version

Speciifica la versione NFS che si desidera utilizzare DataSync per montare la condivisione NFS. Se il server rifiuta di utilizzare la versione specificata, l'attività avrà esito negativo.

Puoi specificare le seguenti opzioni:

- `AUTOMATIC`(impostazione predefinita): DataSync sceglie la versione 4.1 di NFS.
- `NFS3`: versione del protocollo stateless che consente scritture asincrone sul server.
- `NFSv4_0`: versione del protocollo stateful, abilitato per firewall che supporta deleghe e pseudo file system.
- `NFSv4_1`: versione del protocollo stateful che supporta sessioni, deleghe di directory ed elaborazione parallela dei dati. La versione 4.1 di NFS include anche tutte le funzionalità disponibili nella versione 4.0.

> **Note**
>
> DataSync attualmente supporta solo la versione 3 di NFS con sedi Amazon FSx for NetApp ONTAP.

Tipo: stringa

Valori validi: `AUTOMATIC | NFS3 | NFS4_0 | NFS4_1`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++

- AWS SDK per Java V2
- AWS SDK per Ruby V3

OnPremConfig

Gli AWS DataSync agenti che possono connettersi al file server Network File System (NFS).

Indice

AgentArns

Gli Amazon Resource Names (ARNs) degli DataSync agenti che possono connettersi al tuo file server NFS.

Puoi specificare più di un agente. Per ulteriori informazioni, vedere Utilizzo di più DataSync agenti.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Options

Indica come è configurata l'attività di trasferimento. Queste opzioni includono la modalità DataSync di gestione dei file, degli oggetti e dei metadati associati durante il trasferimento. Puoi anche specificare come verificare l'integrità dei dati, impostare limiti di larghezza di banda per l'attività, tra le altre opzioni.

Ogni opzione ha un valore predefinito. A meno che non sia necessario, non è necessario configurare alcuna opzione prima di chiamare StartTaskExecution.

È inoltre possibile sovrascrivere le opzioni dell'attività per ogni esecuzione di attività. Ad esempio, potresti voler modificare il valore `LogLevel` per una singola esecuzione.

Indice

Atime

Speciifica se conservare i metadati che indicano l'ultima volta in cui un file è stato letto o scritto.

> **Note**
>
> Il comportamento di `Atime` non è completamente standard su tutte le piattaforme, quindi è DataSync possibile farlo solo con il massimo impegno.

- `BEST_EFFORT`(impostazione predefinita): DataSync tenta di preservare l'`Atime`attributo originale su tutti i file di origine (ovvero la versione precedente alle `PREPARING` fasi dell'esecuzione dell'attività). Questa opzione è consigliata.
- `NONE`- Ignora. `Atime`

> **Note**
>
> Se `Atime` è impostato su `BEST_EFFORT`, `Mtime` deve essere impostato su `PRESERVE`. Se `Atime` è impostato su `NONE`, anche `Mtime` deve essere `NONE`.

Tipo: stringa

Valori validi: `NONE | BEST_EFFORT`

Campo obbligatorio: no

BytesPerSecond

Limita la larghezza di banda utilizzata da un' DataSync attività. Ad esempio, se desideri DataSync utilizzare un massimo di 1 MB, imposta questo valore su `1048576` (`=1024*1024`).

> **Note**
>
> Non applicabile alle attività in modalità Avanzata.

Tipo: long

Intervallo valido: valore minimo di -1.

Campo obbligatorio: no

Gid

Specifica l'ID di gruppo POSIX (GID) dei proprietari del file.

- `INT_VALUE`(impostazione predefinita): conserva il valore intero dell'ID utente (UID) e del GID, impostazione consigliata.
- `NONE`- Ignora UID e GID.

Per ulteriori informazioni, consulta Comprendere la modalità di gestione dei metadati DataSync di file e oggetti.

Tipo: stringa

Valori validi: `NONE | INT_VALUE | NAME | BOTH`

Campo obbligatorio: no

LogLevel

Speciifica il tipo di log che vengono DataSync pubblicati in un gruppo di log di Amazon CloudWatch Logs. Per specificare il gruppo di log, consulta. CloudWatchLogGroupArn

- `BASIC`- Pubblica i log con solo informazioni di base (come gli errori di trasferimento).
- `TRANSFER`- Pubblica i registri per tutti i file o gli oggetti trasferiti dall' DataSync attività ed esegue controlli di integrità dei dati.

- `OFF`- Non viene pubblicato alcun registro.

Tipo: stringa

Valori validi: `OFF | BASIC | TRANSFER`

Campo obbligatorio: no

Mtime

Specifica se conservare i metadati che indicano l'ultima volta in cui è stato scritto un file prima della `PREPARING` fase di esecuzione dell'attività. Questa opzione è necessaria quando è necessario eseguire un'attività più di una volta.

- `PRESERVE`(impostazione predefinita): conserva l'originale`Mtime`, operazione consigliata.
- `NONE`- Ignora`Mtime`.

> **Note**
>
> Se `Mtime` è impostato su `PRESERVE`, `Atime` deve essere impostato su `BEST_EFFORT`. Se `Mtime` è impostato su `NONE`, anche `Atime` deve essere impostato su `NONE`.

Tipo: stringa

Valori validi: `NONE | PRESERVE`

Campo obbligatorio: no

ObjectTags

Specifica se si desidera DataSync utilizzare i tag come `PRESERVE` oggetto (comportamento predefinito) durante il trasferimento tra sistemi di storage di oggetti. Se desiderate che l' DataSync attività ignori i tag degli oggetti, specificate il `NONE` valore.

Tipo: stringa

Valori validi: `PRESERVE | NONE`

Campo obbligatorio: no

OverwriteMode

Speciifica se DataSync modificare o conservare i dati nella posizione di destinazione.

- `ALWAYS`(impostazione predefinita): DataSync modifica i dati nella posizione di destinazione quando i dati di origine (inclusi i metadati) sono cambiati.

  Se DataSync sovrascrive gli oggetti, potresti incorrere in costi aggiuntivi per determinate classi di storage di Amazon S3 (ad esempio, per il recupero o l'eliminazione anticipata). Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con i trasferimenti Amazon S3.
- `NEVER`- DataSync non sovrascrive i dati nella posizione di destinazione anche se i dati di origine sono cambiati. È possibile utilizzare questa opzione per evitare di sovrascrivere le modifiche apportate a file o oggetti nella destinazione.

Tipo: stringa

Valori validi: `ALWAYS | NEVER`

Campo obbligatorio: no

PosixPermissions

Speciifica quali utenti o gruppi possono accedere a un file per uno scopo specifico, ad esempio la lettura, la scrittura o l'esecuzione del file.

Per ulteriori informazioni, vedere Comprensione della DataSync gestione dei metadati di file e oggetti.

- `PRESERVE`(impostazione predefinita): conserva le autorizzazioni in stile POSIX, operazione consigliata.
- `NONE`- Ignora le autorizzazioni in stile POSIX.

> **Note**
>
> DataSync può conservare le autorizzazioni esistenti di una posizione di origine.

Tipo: stringa

Valori validi: `NONE | PRESERVE`

Campo obbligatorio: no

PreserveDeletedFiles

Speciifica se i file nella posizione di destinazione che non esistono nell'origine devono essere conservati. Questa opzione può influire sui costi di storage di Amazon S3. Se l'attività elimina gli

oggetti, è possibile incorrere in costi minimi per la durata dello storage per determinate classi di storage. Per informazioni dettagliate, consulta Considerazioni sull'utilizzo delle classi di storage Amazon S3 in. DataSync

- `PRESERVE`(impostazione predefinita): ignora tali file di destinazione, operazione consigliata.
- `REMOVE`- Elimina i file di destinazione che non sono presenti nell'origine.

> **Note**
>
> Se imposti questo parametro su`REMOVE`, non puoi `TransferMode` impostarlo `ALL` su. Quando trasferisci tutti i dati, DataSync non analizza la posizione di destinazione e non sa cosa eliminare.

Tipo: stringa

Valori validi: `PRESERVE | REMOVE`

Campo obbligatorio: no

PreserveDevices

Speciifica se DataSync conservare i metadati dei dispositivi a blocchi e a caratteri nella posizione di origine e ricreare i file con quel nome di dispositivo e i metadati nella destinazione. DataSync copia solo il nome e i metadati di tali dispositivi.

> **Note**
>
> DataSync non può copiare il contenuto effettivo di questi dispositivi perché non sono terminali e non restituiscono un marker end-of-file (EOF).

- `NONE`(impostazione predefinita): ignora i dispositivi speciali (consigliato).
- `PRESERVE`- Conserva i caratteri e i metadati dei dispositivi a blocchi. Questa opzione al momento non è supportata per Amazon EFS.

Tipo: stringa

Valori validi: `NONE | PRESERVE`

Campo obbligatorio: no

SecurityDescriptorCopyFlags

Speciifica quali componenti del descrittore di sicurezza SMB vengono copiati dagli oggetti di origine a quelli di destinazione.

Questo valore viene utilizzato solo per i trasferimenti tra le posizioni SMB e Amazon FSx for Windows File Server o tra due posizioni FSx per Windows File Server. Per ulteriori informazioni, consulta Comprendere come DataSync gestisce i metadati di file e oggetti.

- `OWNER_DACL`(impostazione predefinita): per ogni oggetto copiato, DataSync copia i seguenti metadati:
  - Il proprietario dell'oggetto.
  - Liste di controllo degli accessi discrezionali NTFS (DACLs), che determinano se concedere l'accesso a un oggetto.

    DataSync non copierà gli elenchi di controllo degli accessi al sistema NTFS (SACLs) con questa opzione.
- `OWNER_DACL_SACL`- Per ogni oggetto copiato, DataSync copia i seguenti metadati:
  - Il proprietario dell'oggetto.
  - Liste di controllo degli accessi discrezionali NTFS (DACLs), che determinano se concedere l'accesso a un oggetto.
  - SACLs, utilizzati dagli amministratori per registrare i tentativi di accesso a un oggetto protetto.

    La copia SACLs richiede la concessione di autorizzazioni aggiuntive all'utente Windows che DataSync utilizza per accedere alla posizione SMB. Per informazioni sulla scelta di un utente con le autorizzazioni corrette, consulta Autorizzazioni richieste per SMB, per Windows File Server o FSx FSx per ONTAP (a seconda del tipo di posizione nel trasferimento).
- `NONE`- Nessuno dei componenti del descrittore di sicurezza SMB viene copiato. Gli oggetti di destinazione sono di proprietà dell'utente a cui è stato fornito l'accesso alla posizione di destinazione. DACLs e SACLs sono impostati in base alla configurazione del server di destinazione.

Tipo: stringa

Valori validi: `NONE | OWNER_DACL | OWNER_DACL_SACL`

Campo obbligatorio: no

TaskQueueing

Speciifica se le attività di trasferimento devono essere messe in coda in determinati scenari quando si eseguono più attività. Questa è l'impostazione `ENABLED` predefinita.

Tipo: stringa

Valori validi: `ENABLED | DISABLED`

Campo obbligatorio: no

TransferMode

Speciifica se DataSync trasferisce solo i dati (inclusi i metadati) che differiscono tra le posizioni dopo una copia iniziale o trasferisce tutti i dati ogni volta che si esegue l'attività. Se hai intenzione di effettuare trasferimenti ricorrenti, potresti voler trasferire solo le modifiche apportate rispetto alla precedente esecuzione dell'attività.

- `CHANGED`(impostazione predefinita): dopo il trasferimento completo iniziale, DataSync copia solo i dati e i metadati che differiscono tra la posizione di origine e quella di destinazione.
- `ALL`- DataSync copia tutto ciò che si trova nell'origine nella destinazione senza confrontare le differenze tra le posizioni.

Tipo: stringa

Valori validi: `CHANGED | ALL`

Campo obbligatorio: no

Uid

Specifica l'ID utente POSIX (UID) del proprietario del file.

- `INT_VALUE`(impostazione predefinita): conserva il valore intero di UID e ID di gruppo (GID), impostazione consigliata.
- `NONE`- Ignora UID e GID.

Per ulteriori informazioni, vedete Metadati copiati da. DataSync

Tipo: stringa

Valori validi: `NONE | INT_VALUE | NAME | BOTH`

Campo obbligatorio: no

VerifyMode

Speciifica se e come DataSync verifica l'integrità dei dati al termine del trasferimento.

- `ONLY_FILES_TRANSFERRED`(consigliato): DataSync calcola il checksum dei dati trasferiti (inclusi i metadati) nella posizione di origine. Al termine del trasferimento, confronta DataSync quindi questo checksum con il checksum calcolato su quei dati nella destinazione.

  > **Note**
  >
  > Questa è l'opzione predefinita per le attività in modalità Avanzata.

  Consigliamo questa opzione per il trasferimento alle classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con le sedi Amazon S3.
- `POINT_IN_TIME_CONSISTENT`- Al termine del trasferimento, DataSync controlla l'intera origine e la destinazione per verificare che entrambe le sedi siano completamente sincronizzate.

  > **Note**
  >
  > È l'opzione predefinita per le attività in modalità Base e attualmente non è supportata nelle attività in modalità Avanzata.

  Se si utilizza un manifesto, analizza e verifica DataSync solo ciò che è elencato nel manifesto.

  Non puoi utilizzare questa opzione per il trasferimento a classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Per ulteriori informazioni, consulta Considerazioni sulla classe di storage con le sedi Amazon S3.
- `NONE`- DataSync esegue controlli di integrità dei dati solo durante il trasferimento. A differenza di altre opzioni, non è prevista alcuna verifica aggiuntiva al termine del trasferimento.

Tipo: stringa

Valori validi: `POINT_IN_TIME_CONSISTENT | ONLY_FILES_TRANSFERRED | NONE`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Platform

I dettagli relativi alla piattaforma sull' AWS DataSync agente, ad esempio il numero di versione.

Indice

Version

La versione dell'agente. DataSync

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

PrivateLinkConfig

Specifica in che modo l' AWS DataSync agente si connette all' AWS utilizzo di un endpoint del servizio Virtual Private Cloud (VPC). Un agente che utilizza un endpoint VPC non è accessibile sulla rete Internet pubblica.

Indice

PrivateLinkEndpoint

Specifica l'endpoint VPC fornito AWS PrivateLinkdal quale l'agente si connette.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 7. La lunghezza massima è 15 caratteri.

Modello: `\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`

Campo obbligatorio: no

SecurityGroupArns

Speciifica l'Amazon Resource Names (ARN) del gruppo di sicurezza che DataSync fornisce l'accesso all'endpoint VPC. È possibile specificare un solo ARN.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Campo obbligatorio: no

SubnetArns

Speciifica l'ARN della sottorete in cui si trova l'endpoint VPC. È possibile specificare un solo ARN.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/.*$`

Campo obbligatorio: no

VpcEndpointId

Specifica l'ID dell'endpoint VPC a cui l'agente si connette.

Tipo: stringa

Modello: `^vpce-[0-9a-f]{17}$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

QopConfiguration

La configurazione QOP (Quality of Protection) specifica le impostazioni di privacy per le chiamate di procedura remota (RPC, Remote Procedure Call) e per il trasferimento dati configurate nel cluster del file system distribuito Hadoop (HDFS).

Indice

DataTransferProtection

L'impostazione di protezione per il trasferimento dati configurata nel cluster HDFS. Questa impostazione corrisponde all'impostazione `dfs.data.transfer.protection` nel file `hdfs-site.xml` del cluster Hadoop.

Tipo: stringa

Valori validi: `DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY`

Campo obbligatorio: no

RpcProtection

L'impostazione di protezione RPC configurata nel cluster HDFS. Questa impostazione corrisponde all'impostazione `hadoop.rpc.protection` nel file `core-site.xml` del cluster Hadoop.

Tipo: stringa

Valori validi: `DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportDestination

Specificate dove DataSync caricare il rapporto sulle attività.

Indice

S3

Specifica il bucket Amazon S3 DataSync in cui carica il report delle attività.

Tipo: oggetto ReportDestinationS3

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportDestinationS3

Specifica il bucket Amazon S3 DataSync in cui carica il report delle attività.

Indice

BucketAccessRoleArn

Specifica l'Amazon Resource Name (ARN) della policy IAM che DataSync consente di caricare un report delle attività nel bucket S3. Per ulteriori informazioni, consulta Consentire DataSync il caricamento di un report delle attività in un bucket Amazon S3.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Campo obbligatorio: sì

S3BucketArn

Speciifica l'ARN del bucket DataSync S3 in cui carica il rapporto.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 268.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

Campo obbligatorio: sì

Subdirectory

Specificate un prefisso bucket per il rapporto.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportOverride

Specificate il livello di dettaglio per un aspetto particolare del rapporto sulle DataSync attività.

Indice

ReportLevel

Specifica se il rapporto sull'attività include solo errori o successi ed errori.

Ad esempio, il rapporto potrebbe includere principalmente solo ciò che non è andato bene nel trasferimento ()`ERRORS_ONLY`. Allo stesso tempo, vuoi verificare che il filtro delle attività funzioni correttamente. In questa situazione, puoi ottenere un elenco di quali file sono stati ignorati DataSync correttamente e se è stato trasferito qualcosa che non hai trasferito (`SUCCESSES_AND_ERRORS`).

Tipo: stringa

Valori validi: `ERRORS_ONLY | SUCCESSES_AND_ERRORS`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportOverrides

Il livello di dettaglio incluso in ogni aspetto del rapporto sulle DataSync attività.

Indice

Deleted

Speciifica il livello di segnalazione per i file, gli oggetti e le directory che DataSync hanno tentato di eliminare nella posizione di destinazione. Ciò si applica solo se si configura l'attività in modo da eliminare i dati nella destinazione che non si trovano nell'origine.

Tipo: oggetto ReportOverride

Campo obbligatorio: no

Skipped

Speciifica il livello di reporting per i file, gli oggetti e le directory che hai DataSync cercato di ignorare durante il trasferimento.

Tipo: oggetto ReportOverride

Campo obbligatorio: no

Transferred

Speciifica il livello di segnalazione per i file, gli oggetti e le directory che hanno tentato di trasferire. DataSync

Tipo: oggetto ReportOverride

Campo obbligatorio: no

Verified

Speciifica il livello di segnalazione per i file, gli oggetti e le directory che si è DataSync tentato di verificare al termine del trasferimento.

Tipo: oggetto ReportOverride

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportResult

Indica se DataSync è stato creato un rapporto sulle attività completo per il trasferimento.

Indice

ErrorCode

Indica il codice associato all'errore se non è DataSync possibile creare un rapporto completo.

Tipo: string

Campo obbligatorio: no

ErrorDetail

Fornisce dettagli sui problemi relativi alla creazione di un rapporto.

Tipo: string

Campo obbligatorio: no

Status

Indica se DataSync sta ancora lavorando sul rapporto, ha creato un rapporto o non è possibile creare un rapporto completo.

Tipo: stringa

Valori validi: `PENDING | SUCCESS | ERROR`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

S3Config

Speciifica l'Amazon Resource Name (ARN) AWS Identity and Access Management del ruolo DataSync (IAM) utilizzato per accedere al bucket S3.

Per ulteriori informazioni, consulta Fornire l' DataSync accesso ai bucket S3.

Indice

BucketAccessRoleArn

Speciifica l'ARN del ruolo DataSync IAM utilizzato per accedere al bucket S3.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

S3ManifestConfig

Specifica il bucket S3 in cui stai ospitando il manifesto che desideri utilizzare. AWS DataSync Per ulteriori informazioni ed esempi di configurazione, consulta Specificare quali DataSync trasferimenti vengono trasferiti utilizzando un manifesto.

Indice

BucketAccessRoleArn

Specifica il ruolo AWS Identity and Access Management (IAM) che consente di accedere DataSync al manifesto. Per ulteriori informazioni, consulta Fornire DataSync l'accesso al manifesto.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Campo obbligatorio: sì

ManifestObjectPath

Specifica la chiave oggetto Amazon S3 del tuo manifesto. Questo può includere un prefisso (ad esempio,). `prefix/my-manifest.csv`

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 4096.

Modello: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Campo obbligatorio: sì

S3BucketArn

Specifica l'Amazon Resource Name (ARN) del bucket S3 in cui stai ospitando il tuo manifest.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 268.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

Campo obbligatorio: sì

ManifestObjectVersionId

Specificate l'ID della versione dell'oggetto del manifesto che desiderate DataSync utilizzare. Se non lo impostate, DataSync utilizza la versione più recente dell'oggetto.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^.+$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

SmbMountOptions

Speciifica la versione del protocollo Server Message Block (SMB) che viene AWS DataSync utilizzata per accedere a un file server SMB.

Indice

Version

Per impostazione predefinita, sceglie DataSync automaticamente una versione del protocollo SMB in base alla negoziazione con il file server SMB. Puoi anche configurare l'utilizzo DataSync di una versione SMB specifica, ma ti consigliamo di farlo solo se hai problemi a negoziare automaticamente con DataSync il file server SMB.

Di seguito sono riportate le opzioni per la configurazione della versione SMB:

- `AUTOMATIC`(impostazione predefinita): DataSync e il file server SMB negozia la versione più alta di SMB supportata reciprocamente tra la 2.1 e la 3.1.1.

  Questa è la scelta consigliata. Se scegli una versione specifica che il tuo server di file non supporta, potresti ricevere un errore `Operation Not Supported`.
- `SMB3`: limita la negoziazione del protocollo solo alla versione SMB 3.0.2.
- `SMB2`: limita la negoziazione del protocollo solo alla versione 2.1 di SMB.
- `SMB2_0`: limita la negoziazione del protocollo solo alla versione 2.0 di SMB.
- `SMB1`: limita la negoziazione del protocollo solo alla versione 1.0 di SMB.

> **Note**
>
> L'`SMB1`opzione non è disponibile quando si crea una sede Amazon FSx for NetApp ONTAP.

Tipo: stringa

Valori validi: `AUTOMATIC | SMB2 | SMB3 | SMB1 | SMB2_0`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

SourceManifestConfig

Specifica il manifesto che si AWS DataSync desidera utilizzare e dove è ospitato. Per ulteriori informazioni ed esempi di configurazione, vedere Specificazione degli elementi da DataSync trasferire utilizzando un manifesto.

Indice

S3

Specifica il bucket S3 in cui stai ospitando il tuo manifest.

Tipo: oggetto S3ManifestConfig

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TagListEntry

Una coppia chiave-valore che rappresenta un singolo tag applicato a una AWS risorsa.

Indice

Key

La chiave per un tag di AWS risorsa.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:/-]+$`

Campo obbligatorio: sì

Value

Il valore di un tag di AWS risorsa.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskExecutionFilesFailedDetail

Il numero di oggetti che DataSync non vengono preparati, trasferiti, verificati ed eliminati durante l'esecuzione dell'attività.

> **Note**
>
> Si applica solo alle attività in modalità Avanzata.

Indice

Delete

Il numero di oggetti che DataSync non vengono eliminati durante l'esecuzione dell'attività.

Tipo: long

Campo obbligatorio: no

Prepare

Il numero di oggetti che DataSync non vengono preparati durante l'esecuzione dell'attività.

Tipo: long

Campo obbligatorio: no

Transfer

Il numero di oggetti che DataSync non vengono trasferiti durante l'esecuzione dell'attività.

Tipo: long

Campo obbligatorio: no

Verify

Il numero di oggetti che DataSync non viene verificato durante l'esecuzione dell'attività.

Tipo: long

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskExecutionFilesListedDetail

Il numero di oggetti che DataSync trovi nelle tue sedi.

> **Note**
>
> Si applica solo alle attività in modalità Avanzata.

Indice

AtDestinationForDelete

Il numero di oggetti DataSync trovati nella posizione di destinazione. Questo contatore è applicabile solo se si configura l'attività per eliminare i dati nella destinazione che non si trovano nell'origine.

Tipo: long

Campo obbligatorio: no

AtSource

Il numero di oggetti DataSync trovati nella posizione di origine.

- Con un manifesto, DataSync elenca solo ciò che è nel manifesto (e non tutto nella posizione di origine).
- Con un filtro di inclusione, DataSync elenca solo ciò che corrisponde al filtro nella posizione di origine.
- Con un filtro di esclusione, DataSync elenca tutto nella posizione di origine prima di applicare il filtro.

Tipo: long

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskExecutionListEntry

Rappresenta una singola voce in un elenco di esecuzioni di AWS DataSync attività restituite con l'ListTaskExecutionsoperazione.

Indice

Status

Lo stato dell'esecuzione di un'attività. Per ulteriori informazioni, vedere Stati di esecuzione delle attività.

Tipo: stringa

Valori validi: `QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR`

Campo obbligatorio: no

TaskExecutionArn

L'Amazon Resource Name (ARN) dell'esecuzione di un'attività.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|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}$`

Campo obbligatorio: no

TaskMode

La modalità di attività che stai utilizzando. Per ulteriori informazioni, vedere Scelta di una modalità di operazione per il trasferimento dei dati.

Tipo: stringa

Valori validi: `BASIC | ENHANCED`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskExecutionResultDetail

Fornisce informazioni dettagliate sul risultato dell'esecuzione dell' AWS DataSync attività.

Indice

ErrorCode

Un errore che si è DataSync verificato durante l'esecuzione dell'operazione. È possibile utilizzare queste informazioni per risolvere i problemi.

Tipo: string

Campo obbligatorio: no

ErrorDetail

La descrizione dettagliata di un errore DataSync riscontrato durante l'esecuzione dell'attività. È possibile utilizzare queste informazioni per risolvere i problemi.

Tipo: string

Campo obbligatorio: no

PrepareDuration

Il tempo, in millisecondi, durante il quale l'operazione è stata eseguita durante la fase. `PREPARING` Per ulteriori informazioni, vedere Stati di esecuzione delle attività.

Per le attività in modalità Avanzata, il valore è sempre`0`. Per ulteriori informazioni, consulta Come DataSync si prepara il trasferimento dei dati.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: no

PrepareStatus

Lo stato della `PREPARING` fase di esecuzione dell'attività. Per ulteriori informazioni, consulta Stati di esecuzione delle attività.

Tipo: stringa

Valori validi: `PENDING | SUCCESS | ERROR`

Campo obbligatorio: no

TotalDuration

Il tempo in millisecondi in cui è stata eseguita l'esecuzione dell'attività.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: no

TransferDuration

Il tempo in millisecondi durante il quale l'operazione è stata eseguita. `TRANSFERRING` Per ulteriori informazioni, vedere Stati di esecuzione delle attività.

Per le attività in modalità Avanzata, il valore è sempre`0`. Per ulteriori informazioni, consulta Come DataSync trasferisce i dati.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: no

TransferStatus

Lo stato della `TRANSFERRING` fase di esecuzione dell'attività. Per ulteriori informazioni, consulta Stati di esecuzione delle attività.

Tipo: stringa

Valori validi: `PENDING | SUCCESS | ERROR`

Campo obbligatorio: no

VerifyDuration

Il tempo, in millisecondi, durante il quale l'operazione è stata eseguita durante la fase. `VERIFYING` Per ulteriori informazioni, vedere Stati di esecuzione delle attività.

Per le attività in modalità Avanzata, il valore è sempre`0`. Per ulteriori informazioni, consulta Come DataSync verifica l'integrità dei dati.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: no

VerifyStatus

Lo stato della `VERIFYING` fase di esecuzione dell'attività. Per ulteriori informazioni, consulta Stati di esecuzione delle attività.

Tipo: stringa

Valori validi: `PENDING | SUCCESS | ERROR`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskFilter

Puoi utilizzare i filtri API per restringere l'elenco delle risorse restituite da`ListTasks`. Ad esempio, per recuperare tutte le attività in una posizione di origine, è possibile utilizzare `ListTasks` con il nome del filtro `LocationId` e `Operator Equals` con l'ARN per la posizione.

Per ulteriori informazioni, consulta Filtraggio DataSync delle risorse.

Indice

Name

Il nome del filtro utilizzato. Ogni chiamata API supporta un elenco di filtri disponibili. Ad esempio: `LocationId` per `ListTasks`.

Tipo: stringa

Valori validi: `LocationId | CreationTime`

Campo obbligatorio: sì

Operator

L'operatore utilizzato per confrontare i valori dei filtri (ad esempio, `Equals` o`Contains`).

Tipo: stringa

Valori validi: `Equals | NotEquals | In | LessThanOrEqual | LessThan | GreaterThanOrEqual | GreaterThan | Contains | NotContains | BeginsWith`

Campo obbligatorio: sì

Values

I valori in base ai quali si desidera filtrare. Ad esempio, potresti voler visualizzare solo le attività per una località di destinazione specifica.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `^[0-9a-zA-Z_\ \-\:\*\.\\/\?-]*$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskListEntry

Rappresenta una singola voce in un elenco di attività. `TaskListEntry`restituisce un array che contiene un elenco di attività quando viene chiamata l'ListTasksoperazione. Un'attività include i file system di origine e di destinazione da sincronizzare e le opzioni da utilizzare per le attività.

Indice

Name

Il nome dell'attività .

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[a-zA-Z0-9\s+=._:@/-]+$`

Campo obbligatorio: no

Status

Lo stato dell'attività.

Tipo: stringa

Valori validi: `AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE`

Campo obbligatorio: no

TaskArn

L'Amazon Resource Name (ARN) dell'attività.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Campo obbligatorio: no

TaskMode

La modalità attività che stai utilizzando. Per ulteriori informazioni, vedere Scelta di una modalità di operazione per il trasferimento dei dati.

Tipo: stringa

Valori validi: `BASIC | ENHANCED`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskReportConfig

Specifica come si desidera configurare un rapporto sulle attività, che fornisce informazioni dettagliate sul AWS DataSync trasferimento.

Per ulteriori informazioni, consulta Rapporti sulle attività.

Indice

Destination

Specifica il bucket Amazon S3 DataSync in cui carica il report delle attività. Per ulteriori informazioni, consulta Rapporti sulle attività.

Tipo: oggetto ReportDestination

Campo obbligatorio: no

ObjectVersionIds

Specifica se il report delle attività include la nuova versione di ogni oggetto trasferito in un bucket S3. Questo vale solo se abiliti il controllo delle versioni nel tuo bucket. Tieni presente che impostarlo su `INCLUDE` può aumentare la durata dell'esecuzione dell'attività.

Tipo: stringa

Valori validi: `INCLUDE | NONE`

Campo obbligatorio: no

OutputType

Specificate il tipo di rapporto sulle attività che desiderate:

- `SUMMARY_ONLY`: fornisce i dettagli necessari sull'attività, tra cui il numero di file, oggetti e directory trasferiti e la durata del trasferimento.
- `STANDARD`: fornisce dettagli completi sull'attività, incluso un elenco completo di file, oggetti e directory che sono stati trasferiti, ignorati, verificati e altro ancora.

Tipo: stringa

Valori validi: `SUMMARY_ONLY | STANDARD`

Campo obbligatorio: no

Overrides

Personalizza il livello di segnalazione per alcuni aspetti del rapporto sulle attività. Ad esempio, il rapporto potrebbe in genere includere solo errori, ma è possibile specificare che si desidera un elenco di successi ed errori solo per i file che DataSync hanno tentato di eliminare nella posizione di destinazione.

Tipo: oggetto ReportOverrides

Campo obbligatorio: no

ReportLevel

Specificare se si desidera che il rapporto sulle attività includa solo gli errori durante il trasferimento o un elenco di ciò che è riuscito e non è riuscito.

- `ERRORS_ONLY`: Un rapporto mostra ciò che non DataSync è stato possibile trasferire, ignorare, verificare ed eliminare.
- `SUCCESSES_AND_ERRORS`: Un rapporto mostra cosa DataSync è stato possibile e cosa non è stato possibile trasferire, ignorare, verificare ed eliminare.

Tipo: stringa

Valori validi: `ERRORS_ONLY | SUCCESSES_AND_ERRORS`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskSchedule

Configura l' AWS DataSync attività per l'esecuzione in base a una pianificazione (a un intervallo minimo di 1 ora).

Indice

ScheduleExpression

Specificate la pianificazione delle attività utilizzando un'espressione cron o rate.

Utilizza le espressioni cron per le pianificazioni delle attività eseguite in un'ora e in un giorno specifici. Ad esempio, la seguente espressione cron crea una pianificazione delle attività che viene eseguita alle 8:00 del primo mercoledì di ogni mese:

```
cron(0 8 * * 3#1)
```

Utilizza le espressioni di frequenza per le pianificazioni delle attività che vengono eseguite a intervalli regolari. Ad esempio, la seguente espressione di frequenza crea una pianificazione delle attività che viene eseguita ogni 12 ore:

```
rate(12 hours)
```

Per informazioni sulla sintassi delle espressioni cron e rate, consulta la Amazon EventBridge User Guide.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 256.

Modello: `^[a-zA-Z0-9\ \_\*\?\,\|\^\-\/\#\s\(\)\+]*$`

Campo obbligatorio: sì

Status

Specifica se abilitare o disabilitare la pianificazione delle attività. La pianificazione è abilitata per impostazione predefinita, ma in alcuni casi può essere necessario disabilitarla. Ad esempio, potrebbe essere necessario sospendere un trasferimento ricorrente per risolvere un problema relativo all'operazione o eseguire la manutenzione del sistema di storage.

DataSync potrebbe disattivare automaticamente la pianificazione se l'attività fallisce ripetutamente con lo stesso errore. Per ulteriori informazioni, consulta TaskScheduleDetails.

Tipo: stringa

Valori validi: `ENABLED | DISABLED`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TaskScheduleDetails

Fornisce informazioni sulla pianificazione delle AWS DataSync attività.

Indice

DisabledBy

Indica in che modo la pianificazione delle attività è stata disabilitata.

- `USER`- La pianificazione è stata disabilitata manualmente utilizzando l'UpdateTaskoperazione o la DataSync console.
- `SERVICE`- La pianificazione è stata disattivata automaticamente DataSync perché l'attività non è riuscita ripetutamente con lo stesso errore.

Tipo: stringa

Valori validi: `USER | SERVICE`

Campo obbligatorio: no

DisabledReason

Fornisce un motivo se la pianificazione delle attività è disabilitata.

Se la pianificazione è disattivata da`USER`, viene visualizzato un `Manually disabled by user.` messaggio.

Se la tua pianificazione è disattivata da`SERVICE`, viene visualizzato un messaggio di errore che ti aiuta a capire perché l'attività continua a fallire. Per informazioni sulla risoluzione DataSync degli errori, consulta Risoluzione dei problemi relativi ai DataSync trasferimenti.

Tipo: stringa

Vincoli di lunghezza: lunghezza massima di 8192.

Modello: `^[\w\s.,'?!:;\/=|<>()-]*$`

Campo obbligatorio: no

StatusUpdateTime

Indica l'ultima volta in cui lo stato della pianificazione delle attività è cambiato. Ad esempio, se la pianificazione DataSync viene disattivata automaticamente a causa di un errore ripetuto, è possibile vedere quando è stata disabilitata.

Tipo: Timestamp

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Errori comuni

Questa sezione elenca gli errori comuni alle azioni API di tutti i AWS servizi. Per gli errori specifici di un'azione API per questo servizio, consulta l'argomento per quell'azione API.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

IncompleteSignature

La firma della richiesta non è conforme agli AWS standard.

Codice di stato HTTP: 400

InternalFailure

L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto interno sconosciuto.

Codice di stato HTTP: 500

InvalidAction

L'azione o l'operazione richiesta non è valida. Verifica che l'operazione sia digitata correttamente.

Codice di stato HTTP: 400

InvalidClientTokenId

Il certificato X.509 o AWS l'ID della chiave di accesso fornito non esiste nei nostri archivi.

Codice di stato HTTP: 403

NotAuthorized

Non disponi delle autorizzazioni per eseguire questa azione.

Codice di stato HTTP: 400

OptInRequired

L'ID della chiave di AWS accesso richiede un abbonamento al servizio.

Codice di stato HTTP: 403

RequestExpired

La richiesta ha raggiunto il servizio più di 15 minuti dopo la data indicata sulla richiesta o più di 15 minuti dopo la data di scadenza della richiesta (ad esempio nel caso di pre-firmata URLs), oppure la data indicata sulla richiesta è tra più di 15 minuti.

Codice di stato HTTP: 400

ServiceUnavailable

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 503

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

ValidationError

L'input non soddisfa i vincoli specificati da un servizio. AWS

Codice di stato HTTP: 400

Parametri comuni

L'elenco seguente contiene i parametri utilizzati da tutte le azioni per firmare le richieste di Signature Version 4 con una stringa di query. Qualsiasi parametro specifico di un'operazione è riportato nell'argomento relativo all'operazione. Per ulteriori informazioni sulla versione 4 di Signature, consulta Signing AWS API requests nella IAM User Guide.

Action

azione da eseguire.

Tipo: stringa

Campo obbligatorio: sì

Version

La versione dell'API per cui è scritta la richiesta, espressa nel formato YYYY-MM-DD.

Tipo: stringa

Campo obbligatorio: sì

X-Amz-Algorithm

Algoritmo hash utilizzato per creare la firma della richiesta.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Valori validi: `AWS4-HMAC-SHA256`

Obbligatorio: condizionale

X-Amz-Credential

Il valore dell'ambito delle credenziali, che è una stringa che include la chiave di accesso, la data, la regione di destinazione, il servizio richiesto e una stringa di terminazione ("aws4_request"). Il valore viene espresso nel seguente formato: chiave_accesso/AAAAMMGG/regione/servizio/aws4_request.

Per ulteriori informazioni, consulta Creare una richiesta AWS API firmata nella Guida per l'utente IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Date

La data utilizzata per creare la firma. Il formato deve essere il formato di base ISO 8601 (YYYYMMDD'T'HHMMSS'Z'). Per esempio, la data e l'ora seguenti è un X-Amz-Date valore valido:`20120325T120000Z`.

Condizione: X-Amz-Date è facoltativa per tutte le richieste; può essere utilizzata per sovrascrivere la data utilizzata per firmare le richieste. Se l'intestazione Date è specificata nel formato base ISO 8601, non X-Amz-Date è obbligatoria. Quando X-Amz-Date viene utilizzata, sovrascrive sempre il valore dell'intestazione Date. Per ulteriori informazioni, consulta Elementi di una firma di richiesta AWS API nella Guida per l'utente IAM.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Security-Token

Il token di sicurezza temporaneo ottenuto tramite una chiamata a AWS Security Token Service (AWS STS). Per un elenco di servizi che supportano le credenziali di sicurezza temporanee da AWS STS, consulta la pagina Servizi AWS che funzionano con IAM nella Guida per l'utente di IAM.

Condizione: se utilizzi credenziali di sicurezza temporanee di AWS STS, devi includere il token di sicurezza.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Signature

Specifica la firma con codifica esadecimale calcolata dalla stringa da firmare e dalla chiave di firma derivata.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-SignedHeaders

Specifica tutte le intestazioni HTTP incluse come parte della richiesta canonica. Per ulteriori informazioni sulla specificazione delle intestazioni firmate, consulta Creare una richiesta AWS API firmata nella Guida per l'utente IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

Cronologia dei documenti

La tabella seguente descrive importanti aggiunte alla AWS DataSync documentazione. Inoltre, aggiorniamo frequentemente la documentazione per rispondere al feedback che ci inviate.

Per ricevere notifiche sugli aggiornamenti di questa documentazione, iscriviti al feed RSS.

Modifica	Descrizione	Data
Support aggiunto per IPv6 gli indirizzi	Ora puoi utilizzare IPv4 e IPv6 indirizzi per connetterti DataSync e trasferire dati con fonti di dati supportate.	16 luglio 2025
Discovery non è più disponibile	A partire dal 20 maggio 2025, Discovery non è più una DataSync funzionalità disponibile.	20 maggio 2025
AWS aggiornamento della politica gestita: aggiornamento alla politica esistente	La `AWSDataSyncFullAccess` politica ha aggiornato le dichiarazioni di autorizzazione che rimuovono le condizioni di etichettatura dai permessi DataSync utilizzati per creare segreti di Secrets Manager.	13 maggio 2025
AWS aggiornamento della politica gestita: aggiornamento alla politica esistente	La `AWSDataSyncFullAccess` politica dispone di nuove autorizzazioni che consenton o DataSync di utilizzare. AWS Secrets Manager	7 maggio 2025
AWS aggiornamento della politica gestita: aggiornamento alla politica esistente	La `AWSDataSyncFullAccess` politica dispone di nuove autorizzazioni che consenton	23 aprile 2025

	o DataSync di utilizzare. AWS Secrets Manager	
AWS aggiornamento della politica gestita: aggiornamento alla politica esistente	La `AWSDataSyncFullAccess` politica dispone di nuove autorizzazioni che consentono di DataSync lavorare con AWS Secrets Manager e AWS Key Management Service.	23 aprile 2025
AWS aggiornamento della politica gestita: aggiornamento alla politica esistente	`AWSDataSyncServiceRolePolicy` Ha nuove autorizzazioni che consentono di DataSync lavorare con AWS Secrets Manager.	15 aprile 2025
Esecuzione di migrazioni di dati di grandi dimensioni	Scopri come pianificare migrazioni di dati su larga scala utilizzando DataSync per il trasferimento di file o oggetti da un archivio locale o altro cloud a. AWS	19 febbraio 2025
Support per Kerberos con sedi SMB	DataSync ora può utilizzare l'autenticazione Kerberos per la connessione ai file server Server Message Block (SMB).	28 gennaio 2025
Novità Regione AWS	AWS DataSync è disponibile per i trasferimenti di dati nella regione del Messico (Centrale).	14 gennaio 2025
Novità Regione AWS	AWS DataSync è disponibile per i trasferimenti di dati nella regione Asia Pacifico (Tailandia).	7 gennaio 2025

Aggiorna le posizioni AWS di archiviazione	Ora puoi aggiornare le tue sedi di FSx trasferimento Amazon S3, Amazon EFS e Amazon.	18 dicembre 2024
Non supporta più Snowball Edge	A partire dal 12 novembre 2024, DataSync non è più supportato. AWS Snowball Edge	13 novembre 2024
Nuova politica AWS gestita	Il ruolo DataSync collegato al servizio denominato `AWSServiceRoleForDataSync` utilizza una nuova politica gestita denominata. `AWSDataSyncServiceRolePolicy`	30 ottobre 2024
Presentazione della modalità avanzata	Con la modalità Enhanced, puoi trasferire un numero praticamente illimitato di oggetti tra sedi Amazon S3.	30 ottobre 2024
AWS aggiornamenti gestiti delle politiche: aggiornamento a una politica esistente	La `AWSDataSyncFullAccess` politica ha una nuova autorizzazione per i servizi che funzionano con DataSync.	30 ottobre 2024
Support per account Azure v1 di storage generici	DataSync può funzionare con account v1 Azure di storage generici durante il trasferimento da o verso. Microsoft Azure Blob Storage	4 ottobre 2024
Nuovo modo di configurare le pianificazioni delle attività	È possibile configurare le pianificazioni DataSync delle attività utilizzando le espressioni di frequenza.	22 agosto 2024

Novità Regione AWS	AWS DataSync è disponibile per i trasferimenti di dati nella regione Asia Pacifico (Malesia) .	21 agosto 2024
Support per trasferimenti interregionali senza agente che includono una regione opzionale	Non è più necessario un DataSync agente per i trasferimenti tra i servizi di AWS archiviazione quando almeno una posizione di archiviazione è inclusa in un opt-in. Regione AWS	24 luglio 2024
AWS aggiornamenti delle politiche gestite: aggiornamento a una politica esistente	La `AWSDataSyncFullAccess` politica ha una nuova autorizzazione per i servizi che funzionano con DataSync.	22 luglio 2024
Tutorial aggiornato su più account S3	Sono state rimosse alcune autorizzazioni utente dell'account di origine che non sono più necessarie per questo trasferimento.	10 giugno 2024
Nuovo stato di esecuzione dell'attività	Lo `CANCELLING` stato indica quando l'esecuzione di un'attività viene annullata.	15 maggio 2024
Nuova opzione per sospendere la pianificazione delle attività	È possibile disabilitare la pianificazione delle AWS DataSync attività quando è necessario risolvere problemi o eseguire la manutenzione del sistema di storage.	24 aprile 2024

Cifrario TLS aggiornato per endpoint FIPS	AWS DataSync utilizza il codice TLS_AES_128_GCM_SHA256 (secp256r1) per gli endpoint del servizio Federal Information Processing Standard (FIPS).	22 aprile 2024
AWS aggiornamenti delle politiche gestite: aggiornamento a una politica esistente	La `AWSDataSyncFullAccess` politica ha una nuova autorizzazione per i servizi che funzionano con DataSync.	16 febbraio 2024
Trasferisci file o oggetti specifici con un manifesto	AWS DataSync può trasferire un elenco di file o oggetti utilizzando un manifesto.	7 febbraio 2024
Novità Regione AWS	AWS DataSync è ora disponibile per i trasferimenti di dati nella regione Canada occidentale (Calgary).	20 dicembre 2023
Support per trasferimenti con provider cloud aggiuntivi	AWS DataSync ora può trasferire dati tra servizi AWS di archiviazione e IBM Cloud Object Storage oSeagate Lyve Cloud.	7 novembre 2023
Support per trasferimenti con Alibaba Cloud Object Storage Service	AWS DataSync ora può trasferire dati tra servizi AWS di archiviazione eAlibaba Cloud Object Storage Service.	25 settembre 2023
Support per report sulle attività	Monitora AWS DataSync i tuoi trasferimenti con i report sulle attività.	30 agosto 2023

Novità Regione AWS	AWS DataSync è ora disponibile per i trasferimenti di dati nella regione di Israele (Tel Aviv).	23 agosto 2023
Support per trasferimenti con provider cloud aggiuntivi	AWS DataSync ora può trasferire dati tra servizi AWS di archiviazione e diversi altri provider di cloud (come Wasabi Cloud StorageDigitalOcean Spaces, eOracle Cloud Infrastructure Object Storage).	8 agosto 2023
Disponibilità generale del Microsoft Azure Blob Storage supporto	AWS DataSync ora può trasferire oggetti da e versoMicrosoft Azure Blob Storage.	25 luglio 2023
supporto TLS 1.3	Durante il trasferimento tra posizioni di archiviazione, AWS DataSync ora crittografa tutto il traffico di rete con Transport Layer Security (TLS) 1.3.	28 giugno 2023
Nuove metriche Discovery DataSync	DataSync Discovery di AWS ora può dirti quante LUNs (numeri di unità logiche) ci sono in un cluster di risorse di archiviazione, una macchina virtuale di archiviazione (SVM) o un volume.	28 giugno 2023

Novità Regione AWS	AWS DataSync è ora disponibile per i trasferimenti di dati nella regione Asia Pacifico (Melbourne).	24 maggio 2023
Support per lo storage compatibile con S3 su Snowball Edge	È possibile utilizzare AWS DataSync per trasferire dati tra servizi di storage AWS Snowball Edge e AWS servizi di storage compatibili con Amazon S3.	18 maggio 2023
AWS aggiornamenti gestiti delle politiche: aggiornamento a una politica esistente	La `AWSDataSyncFullAccess` politica include nuove autorizzazioni per i servizi che funzionano con DataSync.	2 maggio 2023
Disponibilità generale di DataSync Discovery di AWS	Usa DataSync Discovery per accelerare la migrazione verso AWS.	25 aprile 2023
Versione di anteprima pubblica del supporto per Microsoft Azure Blob Storage	AWS DataSync ora può trasferire oggetti da. Microsoft Azure Blob Storage	29 marzo 2023
Nuova policy IAM	Per supportare la funzionalità DataSync Discovery, DataSync utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForDataSyncDiscovery`	21 marzo 2023
Novità Regioni AWS	AWS DataSync è ora disponibile nei seguenti paesi Regioni AWS: Asia Pacifico (Hyderabad), Europa (Spagna) ed Europa (Zurigo).	6 febbraio 2023

Utilizzo dei tag nelle esecuzioni delle attività	Ora puoi etichettare le esecuzioni delle tue AWS DataSync attività.	16 dicembre 2022
Support per S3 Glacier Instant Retrieval	Ora puoi trasferire oggetti direttamente nella classe di storage S3 Glacier Instant Retrieval.	16 dicembre 2022
Copiare i metadati del sistema a oggetti	AWS DataSync ora può copiare i metadati di sistema durante il trasferimento tra un sistema di storage di oggetti e Amazon S3.	16 dicembre 2022
Novità Regioni AWS	AWS DataSync è ora disponibile nelle regioni Cina (Pechino) e Cina (Ningxia).	14 dicembre 2022
Novità Regione AWS	AWS DataSync è ora disponibile nella regione del Medio Oriente (Emirati Arabi Uniti).	16 novembre 2022
Support per certificati autofirmati con posizioni di archiviazione degli oggetti	AWS DataSync può connettersi a posizioni di archiviazione di oggetti che utilizzano certificati autofirmati o privati.	25 ottobre 2022
Ottieni informazioni sulla compressione dei dati	AWS DataSync può fornire il numero fisico di byte trasferiti sulla rete dopo l'applicazione della compressione.	25 ottobre 2022
Versione di anteprima pubblica di DataSync Discovery di AWS	Usa DataSync Discovery per accelerare la migrazione a AWS.	21 settembre 2022

Nuova opzione per la migrazione dei dati da o verso Google Cloud Storage	Puoi trasferire dati da o verso Google Cloud Storage distribuendo un AWS DataSync agente in Google Cloud.	21 luglio 2022
Support per Amazon FSx per i file system NetApp ONTAP	AWS DataSync ora può trasferire file e cartelle da e verso FSx i file system ONTAP.	28 giugno 2022
Nuove opzioni di sicurezza per le sedi Amazon EFS	AWS DataSync può accedere ai file system Amazon EFS utilizzando TLS, punti di accesso e ruoli IAM.	31 maggio 2022
Migrazione dei dati da o verso Google Cloud Storage e Azure Files	Con AWS DataSync, puoi trasferire dati da o verso Google Cloud Storage e Azure Files. Per ulteriori informazi oni, vedere Creazione di una posizione per l'archiviazione di oggetti e Creazione di una posizione per SMB.	24 maggio 2022
Nuova impostazione AWS DataSync delle attività	Con l'opzione Copia i tag degli oggetti, è possibile specifica re se mantenere i tag degli oggetti durante il trasferimento tra sistemi di archiviazione degli oggetti.	5 maggio 2022
Novità Regione AWS	AWS DataSync è ora disponibi le nella regione Asia Pacifico (Giacarta).	19 aprile 2022

Support per Amazon FSx per i file system OpenZFS	AWS DataSync ora può trasferire file e cartelle da FSx e verso i file system OpenZFS.	5 aprile 2022
Support per i file system Amazon FSx for Lustre	AWS DataSync ora può trasferire file e cartelle da e verso FSx i file system Lustre.	10 dicembre 2021
Support per Hadoop Distributed File System (HDFS)	AWS DataSync ora supporta il trasferimento di file e cartelle da e verso cluster HDFS.	3 novembre 2021
Novità Regione AWS	AWS DataSync è ora disponibile nella regione Asia Pacifico (Osaka).	28 luglio 2021
Trasferimenti completamente automatizzati tra servizi AWS di storage	AWS DataSync ora può trasferire file o oggetti tra Amazon S3, Amazon EFS o FSx Windows File Server con pochi clic nella console. DataSync	9 novembre 2020
Regolazione della larghezza di banda di rete utilizzata da un'attività in esecuzione	AWS DataSync ora consente ai clienti di regolare la larghezza di banda di rete utilizzata da un'attività in esecuzione. DataSync Ciò consente di ridurre al minimo l'impatto su altri utenti o applicazioni quando un'attività si protrae per più giorni.	9 novembre 2020
Supporto avanzato per le funzioni delle macchine DataSync virtuali (VM) locali	La console host VM dell' AWS DataSync agente ora supporta funzioni avanzate, inclusa l'attivazione di un agente dalla console locale.	19 ottobre 2020

AWS DataSync ora può trasferire dati da e verso AWS Outposts	DataSync ora supporta il trasferimento di oggetti da e verso Amazon AWS Outposts S3 in poi.	30 settembre 2020
Support per il filtraggio delle API	AWS DataSync ora supporta il filtraggio per le chiamate `ListTasks` e le chiamate `ListLocations` API, consentendoti di recuperare facilmente la configurazione delle attività di trasferimento dei dati utilizzando filtri come l'origine o la destinazione del trasferimento dei dati.	18 agosto 2020
Support per la copia dei dati dallo storage di oggetti autogestito	AWS DataSync ora supporta il trasferimento di dati tra lo storage di oggetti autogesti to e Amazon S3, Amazon Elastic File System FSx o per Windows File Server.	27 luglio 2020
Support per Linux Kernel-ba sed Virtual Machine (KVM) e hypervisor Microsoft Hyper-V	AWS DataSync ora offre la possibilità di implementare agenti locali sulle piattafor me di virtualizzazione KVM e Microsoft Hyper-V, oltre alle opzioni esistenti e Amazon. VMware EC2	1 luglio 2020

AWS DataSync ora puoi configurare automaticamente la configurazione di Amazon CloudWatch Logs	Quando lo utilizzi DataSync, ora hai la possibilità di generare automaticamente i gruppi di CloudWatch log e la politica delle risorse necessari per pubblicare i log per il trasferimento dei dati, semplificando la creazione delle attività e la configura zione del monitoraggio.	1 luglio 2020
AWS DataSync ora può trasferire dati da e verso AWS Snowball Edge	DataSync ora supporta il trasferimento di file da AWS Snowball Edge e verso il componente più piccolo dei dispositivi AWS Snow Family di edge computing e trasferim ento dati. Snowball Edge è portatile, robusto e sicuro, così piccolo e leggero da stare in uno zaino e in grado di resistere agli ambienti più ostili.	17 giugno 2020
Novità Regione AWS	AWS DataSync è ora disponibi le nella regione Africa (Città del Capo) e nella regione Europa (Milano).	16 giugno 2020
Funzionalità di monitoraggio avanzate con registrazione a livello di file	Ora puoi abilitare la registraz ione dettagliata di file e oggetti copiati tra server NFS, server SMB, bucket Amazon S3, file system Amazon EFS e FSx file system Windows File Server.	24 aprile 2020

Support per la copia di dati tra la tua condivisione SMB e Amazon FSx for Windows File Server	Ora puoi copiare i dati tra la tua condivisione SMB e FSx per Windows File Server.	24 gennaio 2020
Support per la pianificazione delle attività	È ora possibile eseguire manualmente le attività o pianificarle per l'esecuzione in base a un piano specifico.	20 novembre 2019
Novità Regione AWS	AWS DataSync è ora disponibile nella regione Asia Pacifico (Hong Kong), nella regione Asia Pacifico (Mumbai), nella regione Europa (Stoccolma), nella regione del Sud America (San Paolo) e nella regione AWS GovCloud (Stati Uniti orientali).	20 novembre 2019
Novità Regione AWS	AWS DataSync è ora disponibile nella regione Canada (Centrale), nella regione Europa (Londra) e nella regione Europa (Parigi).	2 ottobre 2019
Support per le classi di storage Amazon S3	Ora puoi trasferire oggetti direttamente nelle classi di storage Amazon S3.	24 settembre 2019
Novità Regione AWS	AWS DataSync è ora disponibile nella regione Medio Oriente (Bahrein).	28 agosto 2019
Supporto per la copia dei dati tra la condivisione Server Message Block (SMB) e Amazon S3 o Amazon EFS	Ora puoi copiare i dati tra la tua condivisione di file SMB e Amazon S3 o Amazon EFS.	22 agosto 2019

Support per l'utilizzo di endpoint VPC (Virtual Private Cloud)	Ora puoi creare una connessione privata tra il tuo agente AWS ed eseguire attività in una rete privata. Questo consente di incrementare la sicurezza dei dati poiché vengono copiati sulla rete.	5 agosto 2019
Supporto per gli endpoint Federal Information Processing Standard (FIPS)	Ora puoi utilizzare gli endpoint FIPS per creare agenti ed eseguire attività.	5 agosto 2019
Novità Regione AWS	AWS DataSync è ora disponibile nella regione AWS GovCloud (Stati Uniti occidentali).	11 giugno 2019
Support per il filtraggio	Ora puoi applicare filtri per trasferire solo un sottoinsieme dei file nel percorso di origine quando trasferisci dati dalla posizione di origine a quella di destinazione.	22 maggio 2019
Prima versione di AWS DataSync	Versione generale del AWS DataSync servizio.	26 novembre 2018

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.