aws

사용 설명서

AWS DataSync



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

AWS DataSync: 사용 설명서

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

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

AWS DataSync란 무엇인가요? 1
사용 사례 2
이점 2
추가 리소스 3
작동 방식 4
DataSync 전송 아키텍처 4
온프레미스 스토리지와 간 전송 AWS 4
AWS 스토리지 서비스 간 전송 5
AWS 스토리지 서비스와 다른 클라우드의 스토리지 시스템 간 전송 6
개념 및 용어 7
에이전트 7
Location 7
Task 7
작업 실행 7
DataSync가 파일, 객체, 디렉터리를 전송하는 방법 8
DataSync가 데이터 전송을 준비하는 방법 8
DataSync가 데이터를 전송하는 방법 9
DataSync가 데이터 무결성을 확인하는 방법 9
DataSync가 열린 파일 및 잠긴 파일을 처리하는 방법 10
반복 전송 옵션 10
시작하기 11
에 가입 AWS 계정 11
관리자 액세스 권한이 있는 사용자 생성 11
DataSync 사용 시 필요한 IAM 권한 12
AWS 관리형 정책 13
고객 관리형 정책 13
DataSync는 어디에 사용할 수 있나요? 13
DataSync를 어떻게 사용할 수 있나요? 13
DataSync의 비용은 얼마일까요? 14
DataSync가 사용하는 오픈 소스 구성 요소 14
에이전트가 필요합니까? 14
DataSync 에이전트가 필요한 상황 14
DataSync 에이전트가 필요하지 않은 상황 14
작업 모드에 대한 에이전트 선택 15

여러 DataSync 에이전트 사용 15
다음 단계 16
에이전트 요구 사항 16
하이퍼바이저 요구 사항 16
DataSync 전송을 위한 에이전트 요구 사항 17
AWS 리전 파티션에 대한 에이전트 요구 사항 19
에이전트 관리 요구 사항 19
에이전트 배포 19
VMware에 에이전트 배포 19
KVM에 에이전트 배포 20
Microsoft Hyper-V에 기본 모드 에이전트 배포 21
Amazon EC2 에이전트 배포 22
에 기본 모드 에이전트 배포 AWS Outposts 27
에이전트용 서비스 엔드포인트 선택 27
퍼블릭 서비스 엔드포인트 선택 28
FIPS 서비스 엔드포인트 선택 28
VPC 서비스 엔드포인트 선택 28
에이전트 활성화 31
사전 조건 31
활성화 키 가져오기 32
에이전트 활성화 34
다음 단계 37
에이전트의 네트워크 연결 확인 37
에이전트의 로컬 콘솔 액세스 37
에이전트의 스토리지 시스템 연결 확인 38
에이전트의 DataSync 서비스 연결 확인 39
다음 단계 39
네트워크 연결 40
1. 스토리지 시스템과 에이전트 간의 네트워크 연결 40
2. 에이전트와 DataSync 서비스 간의 네트워크 연결 40
에 스토리지 네트워크 연결 AWS 41
서비스 엔드포인트 선택 41
3. DataSync 서비스와 AWS 스토리지 서비스 간의 네트워크 연결 41
DataSync 에이전트가 필요하지 않은 경우의 네트워킹 41
DataSync 트래픽이 네트워크를 통과하는 방식 및 위치 42
DataSync의 네트워크 보안 42

네트워크 요구 사항 42
IPv6 지원 42
온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항 43
AWS 스토리지 서비스에 대한 네트워크 요구 사항 48
퍼블릭 또는 FIPS 서비스 엔드포인트의 네트워크 요구 사항 48
VPC 또는 FIPS VPC 서비스 엔드포인트에 대한 네트워크 요구 사항 56
데이터 전송을 위한 네트워크 인터페이스 59
에이전트와의 전송을 위한 네트워크 인터페이스 59
에이전트 없이 전송을 위한 네트워크 인터페이스 60
네트워크 인터페이스 보기 61
Direct Connect를 사용한 아키텍처 및 라우팅 예제 61
DataSync VPC 서비스 엔드포인트에서 Direct Connect 사용 62
DataSync 퍼블릭 또는 FIPS 서비스 엔드포인트에서 Direct Connect 사용 65
다음 단계 65
여러 개의 NIC에 대한 에이전트 구성 66
데이터 전송 67
데이터를 어디로 전송할 수 있나요? 68
동일한에서 지원되는 전송 AWS 계정 68
에서 지원되는 전송 AWS 계정 69
동일한에서 지원되는 전송 AWS 리전 71
간 지원되는 전송 AWS 리전 71
전송에 DataSync 에이전트가 필요한지 여부 확인 71
온프레미스 스토리지와 전송 71
NFS 파일 서버로 전송 구성 72
SMB 파일 서버로 전송 구성 76
HDFS 클러스터를 사용하여 전송 구성 86
객체 스토리지 시스템을 사용한 전송 구성 90
AWS 스토리지로 또는 스토리지에서 전송 94
Amazon S3를 사용하여 전송 구성하기 95
Amazon EFS를 사용하여 전송 구성하기 125
FSx for Windows File Server를 사용하여 전송 구성 133
FSx for Lustre를 사용하여 전송 구성 138
FSx for OpenZFS를 사용하여 전송 구성 140
FSx for ONTAP를 사용하여 전송 구성 144
다른 클라우드 스토리지로 간 전송 151
타사 클라우드 스토리지 시스템과 전송 계획 151

Google Cloud Storage로 전송 구성 153
Microsoft Azure Blob Storage를 사용하여 전송 구성 162
Microsoft Azure Files를 사용하여 전송 구성 179
다른 클라우드 객체 스토리지를 사용한 전송 구성 182
데이터 전송을 위한 작업 생성 188
작업 생성 188
태스크 상태 191
여러 작업으로 대규모 데이터세트 파티셔닝 191
여러 작업을 사용하여 전송된 데이터 분할 192
전송을 위한 작업 모드 선택 192
전송할 데이터 선택 196
데이터 무결성 확인 233
대역폭 제한 설정 235
사용자 작업 예약 237
태스크 태그 지정 241
데이터 전송 작업 시작 244
태스크 시작하 245
태스크 실행 상태 246
작업이 대기열에 있는 시점 파악 247
작업 실행 취소 247
데이터 전송 모니터링 249
데이터 전송 성능 카운터 이해 249
CloudWatch 지표를 사용한 데이터 전송 모니터링 267
DataSync를 위한 CloudWatch 지표 268
작업 보고서로 데이터 전송 모니터링 271
사용 사례 271
요약 전용 작업 보고서 271
표준 작업 보고서 272
작업 보고서 예제 275
제한 사항 278
작업 보고서 생성 278
작업 보고서 보기 288
CloudWatch Logs를 사용하여 데이터 전송 모니터링 288
DataSync가 CloudWatch 로그 그룹에 로그를 업로드하도록 허용 289
DataSync 작업에 대한 로깅 구성 291
DataSync 작업 로그 보기 293

CloudTrail을 사용하여 로깅 295
CloudTrail에서의 DataSync 정보 작업 295
DataSync 로그 파일 항목의 이해 296
EventBridge로 모니터링 298
DataSync 전송 이벤트 298
수동 도구를 사용한 모니터링 300
DataSync 콘솔을 사용하여 전송 모니터링 300
를 사용하여 전송 모니터링 AWS CLI 300
watch 유틸리티를 사용하여 전송 모니터링 302
리소스 관리 303
DataSync 에이전트 관리 303
DataSync 에이전트의 연결 및 시스템 리소스 테스트 303
DataSync 에이전트 교체 303
DataSync 리소스 정리 303
DataSync 에이전트의 인프라 재사용 303
에이전트 관리 303
에이전트 소프트웨어 업데이트 303
에이전트 상태 304
에이전트 문제 해결 305
에이전트에 대한 유지 관리 수행 305
에이전트의 로컬 콘솔 액세스 305
에이전트의 DHCP, DNS, IP 설정 구성 307
에이전트의 시스템 리소스 점검 311
에이전트 시스템 시간 서버 구성 보기 및 관리 312
에이전트에 대한 유지 관리 관련 명령 실행 313
상담원 교체하기 314
새 에이전트 만들기 315
새 에이전트를 통한 위치 업데이트 315
다음 단계 320
DataSync 리소스 필터링 320
필터링을 위한 파라미터 321
위치별 필터링 322
작업 기준으로 필터링 323
DataSync 리소스 정리 324
DataSync 에이전트 삭제 324
DataSync 에이전트의 인프라 재사용 325

DataSync 위치 삭제 325
DataSync 작업 삭제 325
보안 327
데이터 보호 327
전송 중 암호화 328
저장 시 암호화 331
인터네트워크 트래픽 개인 정보 332
ID 및 액세스 관리 332
액세스 관리 333
AWS 관리형 정책 338
고객 관리형 정책 344
서비스 연결 역할 사용 347
생성 시 리소스 태그 지정 351
교차 서비스 혼동된 대리인 방지 352
규정 준수 확인 354
복원성 354
인프라 보안 355
스토리지 위치 자격 증명 보호 355
기본 키로 암호화된 서비스 관리형 보안 암호 사용 356
사용자 지정 AWS KMS 키로 암호화된 서비스 관리형 보안 암호 사용 356
사용자가 관리하는 보안 암호 사용 358
할당량 361
스토리지 시스템, 파일, 객체 제한 361
DataSync 할당량 361
할당량 증가 요청 366
문제 해결 367
에이전트 문제 해결 367
Amazon EC2 에이전트의 로컬 콘솔에 연결하려면 어떻게 해야 합니까? 367
에이전트 활성화 키 검색 실패 오류는 무엇을 의미하나요? 368
여전히 VPC 서비스 엔드포인트를 사용하여 에이전트를 활성화할 수 없습니다. 368
에이전트가 오프라인 상태인 경우, 어떻게 해야 하나요? 368
상담원에게 무슨 일이 벌어지고 있는지 모르겠어요. 누군가 저를 도와줄 수 있나요? 369
위치 문제 해결 370
NFS 권한 거부 오류가 발생하여 작업 실패 370
NFS 탑재 오류가 발생하여 작업 실패 370
Amazon EFS 탑재 오류로 작업 실패 371

NFS 전송으로 파일 소유권이 유지되지 않음 371
작업이 Kerberos를 사용하는 SMB 위치에 액세스할 수 없음 372
입력/출력 오류로 작업이 실패했습니다. 373
오류: FsS3UnableToConnectToEndpoint 374
오류: FsS3HeadBucketFailed 374
Unable to list Azure Blobs on the volume root 오류가 발생하여 작업 실패 ... 374
오류: FsAzureBlobVolRootListBlobsFailed 375
오류: SrcLocHitAccess 375
오류: SyncTaskErrorLocationNotAdded 375
오류: S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation 375
HeadObject 또는 GetObjectTagging 오류와 함께 S3 소스 위치에서 작업 실패 376
작업 문제 해결 376
오류: 동기화 옵션 값이 잘못되었습니다. 옵션: TransferMode,PreserveDeletedFiles, 값: ALL,REMOVE 376
EniNotFound 오류와 함께 작업 실행 실패 377
메모리를 할당할 수 없음 오류와 함께 작업 실행 실패 377
FSx for ONTAP 파일 시스템에서 Input/Output error와 함께 작업 실패 378
FSx for ONTAP 파일 시스템에 대한 Connection Reset by peer 또는 Host is down 메시지와 함께 작업 실패 379
작업 실행이 시작 상태이지만 아무 일도 일어나지 않음 380
작업 실행이 준비 상태에서 중단됨 380
전송 완료 전 작업 실행이 중지됨 381
Google Cloud Storage 버킷에서 전송 시 작업 실행 실패 381
작업 실행 타임스탬프 간 불일치 381
NoMem 오류가 발생하여 작업 실행 실패 382
FsNfsIdMappingEnabled 오류가 발생하여 작업 실행 실패 382
객체가 user metadata key 오류로 Azure Blob Storage로 전송되지 않음 382
대상 위치에 /.aws-datasync 폴더가 있음 382
SMB를 사용하여 위치 간에 심볼 링크를 전송할 수 없음 382
작업 보고서 오류 383
데이터 확인 문제 해결 383
파일 콘텐츠 간에 불일치가 있습니다. 383
파일의 SMB 메타데이터 간에 불일치가 있습니다. 384
전송할 파일이 현재 소스 위치에 없음 385
DataSync가 대상 데이터를 확인할 수 없음 386

DataSync가 객체 메타데이터를 읽을 수 없음 ... 387
객체의 시스템 정의 메타데이터 불일치 ... 388
데이터 확인 기간 이해 ... 389
DataSync를 사용한 S3 스토리지 비용 문제 해결 ... 389
자습서 ... 391
계정 간 온프레미스에서 S3로 전송 ... 391
개요 ... 391
사전 조건: 필수 소스 계정 권한 ... 392
사전 조건: 필수 대상 계정 권한 ... 395
1단계: 소스 계정에서 DataSync 에이전트를 생성합니다. ... 395
2단계: 소스 계정에서 대상 버킷 액세스의 DataSync IAM 역할 생성 ... 395
3단계: 대상 계정에서 S3 버킷 정책 업데이트 ... 398
4단계: 목적지 계정에서 S3 버킷의 ACL을 비활성화합니다. ... 399
5단계: 소스 계정에서 온프레미스 스토리지를 위한 DataSync 소스 위치 생성 ... 400
6단계: 소스 계정에서 S3 버킷의 DataSync 목적지 위치를 생성합니다. ... 400
7단계: 소스 계정에서 DataSync 전송 작업을 생성하고 시작 ... 401
관련 리소스 ... 401
계정의 S3 버킷 간 전송 ... 402
개요 ... 402
사전 조건: 필수 소스 계정 권한 ... 404
사전 조건: 필수 대상 계정 권한 ... 407
1단계: 소스 계정에서 대상 버킷 액세스의 DataSync IAM 역할 생성 ... 407
2단계: 대상 계정에서 S3 버킷 정책 업데이트 ... 409
3단계: 대상 계정에서 S3 버킷의 ACL을 비활성화합니다. ... 411
4단계: 소스 계정에서 DataSync 위치 생성 ... 411
5단계: 소스 계정에서 DataSync 전송 작업을 생성하고 시작 ... 413
문제 해결 ... 414
관련: 서버 측 암호화를 사용하여 S3 버킷으로 교차 계정 전송 ... 413
대규모 마이그레이션 수행 ... 415
대규모 데이터 마이그레이션이란 무엇인가요? ... 415
대규모 데이터 마이그레이션의 주요 단계 ... 415
추가 리소스 ... 416
1단계: 마이그레이션 계획 ... 416
요구 사항 수집 ... 417
개념 증명 실행 ... 422
마이그레이션 타임라인 추정 ... 424

2단계: 마이그레이션 구현 426
파티셔닝을 사용하여 마이그레이션 가속화 426
DataSync 작업 실행 428
전송 모니터링 429
데이터싱크 API 431
작업 431
CancelTaskExecution 434
CreateAgent 436
CreateLocationAzureBlob 441
CreateLocationEfs 447
CreateLocationFsxLustre 453
CreateLocationFsxOntap 457
CreateLocationFsxOpenZfs 462
CreateLocationFsxWindows 467
CreateLocationHdfs 473
CreateLocationNfs 481
CreateLocationObjectStorage 486
CreateLocationS3 493
CreateLocationSmb 498
CreateTask 507
DeleteAgent 516
DeleteLocation 518
DeleteTask 520
DescribeAgent 522
DescribeLocationAzureBlob 527
DescribeLocationEfs 532
DescribeLocationFsxLustre 537
DescribeLocationFsxOntap 540
DescribeLocationFsxOpenZfs 545
DescribeLocationFsxWindows 549
DescribeLocationHdfs 554
DescribeLocationNfs 560
DescribeLocationObjectStorage 564
DescribeLocationS3 569
DescribeLocationSmb 574
DescribeTask 581

DescribeTaskExecution 590
ListAgents 611
ListLocations 614
ListTagsForResource 617
ListTaskExecutions 620
ListTasks 623
StartTaskExecution 626
TagResource 633
UntagResource 636
UpdateAgent 639
UpdateLocationAzureBlob 641
UpdateLocationEfs 646
UpdateLocationFsxLustre 650
UpdateLocationFsxOntap 653
UpdateLocationFsxOpenZfs 656
UpdateLocationFsxWindows 659
UpdateLocationHdfs 663
UpdateLocationNfs 669
UpdateLocationObjectStorage 672
UpdateLocationS3 678
UpdateLocationSmb 682
UpdateTask 689
UpdateTaskExecution 695
데이터 타입 697
AgentListEntry 700
AzureBlobSasConfiguration 702
CmkSecretConfig 703
CustomSecretConfig 705
Ec2Config 707
FilterRule 709
FsxProtocol 710
FsxProtocolNfs 711
FsxProtocolSmb 712
FsxUpdateProtocol 715
FsxUpdateProtocolSmb 716
HdfsNameNode 718

LocationFilter 719
LocationListEntry 721
ManagedSecretConfig 723
ManifestConfig 724
NfsMountOptions 726
OnPremConfig 727
Options 728
Platform 736
PrivateLinkConfig 737
QopConfiguration 739
ReportDestination 740
ReportDestinationS3 741
ReportOverride 743
ReportOverrides 744
ReportResult 746
S3Config 747
S3ManifestConfig 748
SmbMountOptions 750
SourceManifestConfig 752
TagListEntry 753
TaskExecutionFilesFailedDetail 754
TaskExecutionFilesListedDetail 756
TaskExecutionFoldersFailedDetail 758
TaskExecutionFoldersListedDetail 760
TaskExecutionListEntry 762
TaskExecutionResultDetail 764
TaskFilter 767
TaskListEntry 769
TaskReportConfig 771
TaskSchedule 773
TaskScheduleDetails 775
일반적인 오류 유형 776
공통 파라미터 778
문서 이력 781
AWS 용어집 794
..... dccxcv

AWS DataSync란 무엇인가요?

AWS DataSync 는 스토리지 서비스 간에 AWS 파일 또는 객체 데이터를 빠르고 쉽게 전송할 수 있는 안전하고 안정적인 고속 파일 전송 서비스입니다.

온프레미스 스토리지 전송

DataSync는 다음과 같은 온프레미스 스토리지 시스템에서 작동합니다.

- NFS(Network File System)
- SMB(Server Message Block)
- Hadoop 분산 파일 시스템(HDFS)
- 객체 스토리지

AWS 스토리지 전송

DataSync는 다음 AWS 스토리지 서비스와 함께 작동합니다.

- Amazon S3
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP

기타 클라우드 스토리지 전송

DataSync는 다음과 같은 다른 클라우드의 스토리지 서비스와 함께 작동합니다.

- 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

사용 사례

다음은 DataSync에 대한 주요 사용 사례의 일부입니다.

- 데이터 마이그레이션 - 네트워크를 통해 활성 데이터 세트를 AWS 스토리지 서비스로 빠르게 전송합니다. DataSync는 데이터를 즉시 사용할 수 있도록 손상 없이 안전하게 전송하기 위해 자동 암호화 및 데이터 무결성 검증을 포함합니다.
- 콜드 데이터 보관 - 온프레미스 스토리지에 저장된 콜드 데이터를 S3 Glacier Flexible Retrival 또는 S3 Glacier Deep Archive와 같은 내구성이 뛰어나고 안전한 장기 스토리지 클래스로 직접 이동합니다. 이렇게 하면 온프레미스 스토리지 용량을 확보하고 레거시 시스템을 종료하는 데 도움이 될 수 있습니다.
- 데이터 복제 - 데이터를 대부분의 Amazon S3 스토리지 클래스에 복사하여 필요에 가장 비용 효율적인 스토리지 클래스를 선택합니다. 대기 파일 시스템을 위해 Amazon EFS 또는 Amazon FSx로 데이터를 전송할 수도 있습니다.
- 클라우드 내 처리를 위한 데이터 전송 - 처리를 AWS 위해 데이터를 내부 또는 외부로 전송합니다. 이러한 접근 방법은 많은 산업 분야에서 중요한 하이브리드 클라우드 워크플로우를 가속화할 수 있습니다. 이러한 워크플로우는 생명 과학 분야의 기계 학습, 미디어 및 엔터테인먼트의 비디오 제작, 재무 분야의 빅 데이터 분석, 석유 및 가스 분야의 지진 연구 등을 포함합니다.

이점

DataSync를 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 데이터 이동 자동화 - DataSync를 사용하면 네트워크를 통해 스토리지 시스템과 서비스 간에 데이터를 더 쉽게 전송할 수 있습니다. DataSync는 고성능의 안전한 데이터 전송에 필요한 데이터 전송 프로세스 및 인프라 관리를 자동화합니다.
- 안전한 데이터 전송 - DataSync는 암호화 및 무결성 검증을 포함한 엔드 투 엔드 보안을 제공하여 데이터를 안전하게, 손상 없이, 즉시 사용할 수 있는 상태로 도착하도록 보장합니다. DataSync는 AWS

Identity and Access Management (IAM) 역할과 같은 내장 AWS 보안 메커니즘을 통해 AWS 스토리지에 액세스합니다. 또한 가상 Virtual Private Cloud(VPC) 엔드포인트를 지원하여 공용 인터넷을 거치지 않고 데이터를 전송할 수 있는 옵션을 제공하고 온라인으로 복사된 데이터의 보안을 더욱 강화합니다.

- 더 빠른 데이터 이동 - DataSync는 특별히 구축된 네트워크 프로토콜과 병렬 멀티스레드 아키텍처를 사용하여 전송을 가속화합니다. 이러한 접근 방법을 통해 마이그레이션, 분석 및 기계 학습을 위한 반복적 데이터 프로세싱 워크플로우 그리고 데이터 보호 프로세스가 가속화됩니다.

추가 리소스

다음 내용을 읽어보면 도움이 됩니다.

- DataSync 리소스 - 블로그, 동영상, 기타 교육 자료 포함
- AWS re:Post – DataSync에 대한 최신 토론 보기
- AWS DataSync 요금

AWS DataSync 작동 방식

온프레미스 및 클라우드 위치에서 데이터를 전송하는 방법을 포함하여 AWS DataSync 전송과 관련된 주요 개념과 용어를 알아봅니다.

DataSync 전송 아키텍처

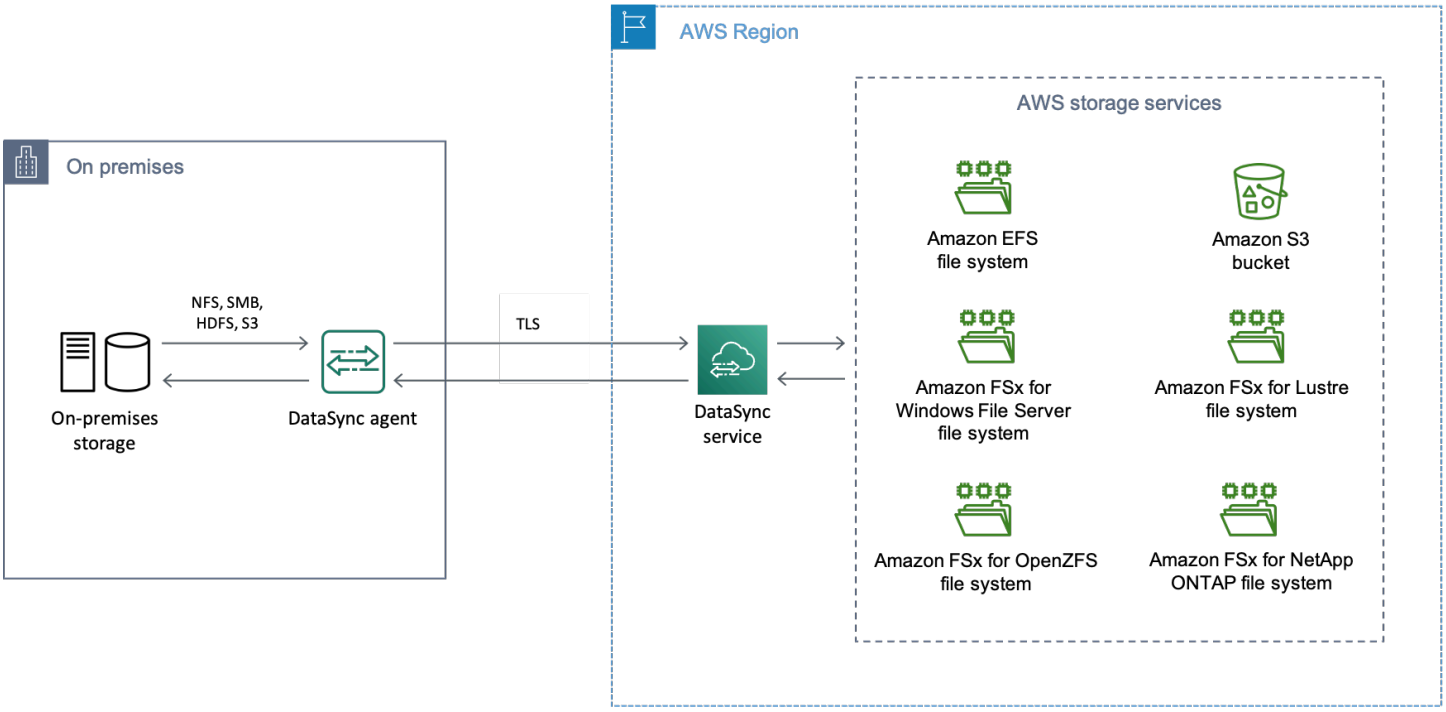
다음 다이어그램은 DataSync의 일반적인 스토리지 데이터 전송 방법과 위치를 보여줍니다. DataSync 지원 스토리지 시스템 및 서비스의 전체 목록은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.

주제

- 온프레미스 스토리지와 간 전송 AWS
- AWS 스토리지 서비스 간 전송
- AWS 스토리지 서비스와 다른 클라우드의 스토리지 시스템 간 전송

온프레미스 스토리지와 간 전송 AWS

다음 다이어그램은 자체 관리형 온프레미스 스토리지 시스템과 간에 파일을 전송하는 DataSync에 대한 개략적인 개요를 보여줍니다 AWS 서비스.

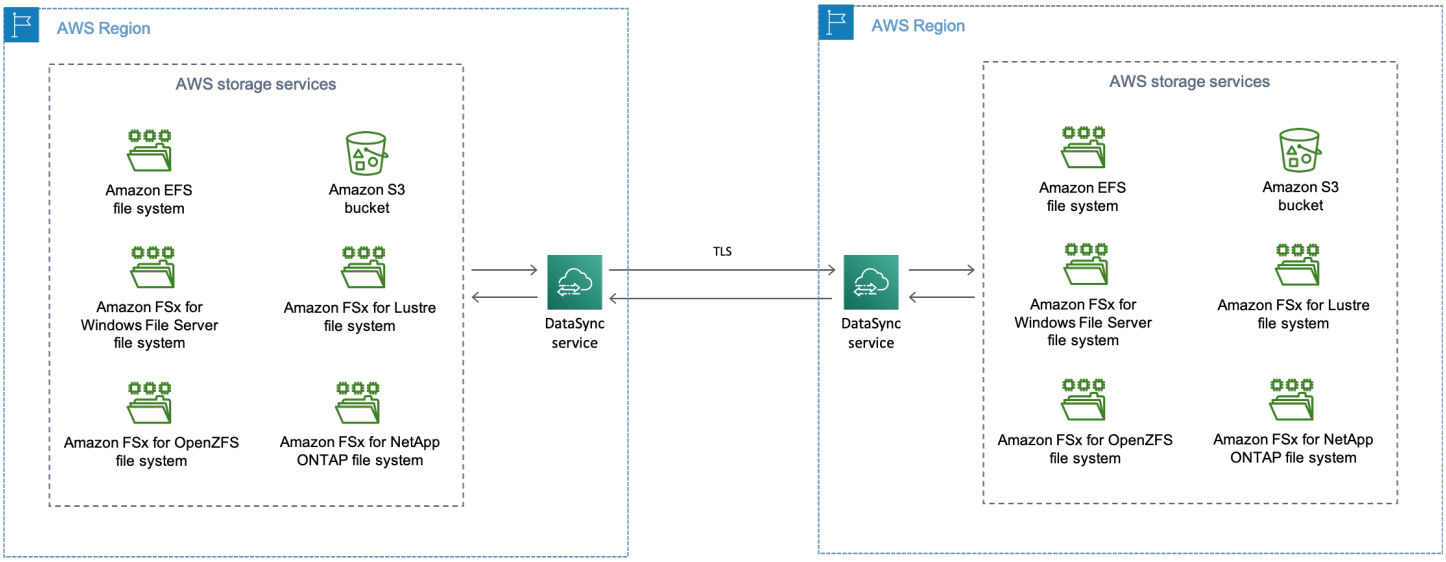


도표는 일반적인 DataSync 사용 사례를 보여줍니다.

- 온프레미스 스토리지 시스템에서 데이터를 복사하는 DataSync 에이전트입니다.
- 전송 계층 보안(TLS)을 사용하여 AWS암호화된 데이터로 이동합니다.
- DataSync는 지원되는 AWS 스토리지 서비스에 데이터를 복사합니다.

AWS 스토리지 서비스 간 전송

다음 다이어그램은 동일한의 간에 파일을 전송하는 DataSync AWS 서비스 에 대한 개략적인 개요를 보여줍니다 AWS 계정.



도표는 일반적인 DataSync 사용 사례를 보여줍니다.

- DataSync는 지원되는 AWS 스토리지 서비스에서 데이터를 복사합니다.
- TLS를 사용하여 AWS 리전암호화된 데이터 이동.
- DataSync는 지원되는 AWS 스토리지 서비스에 데이터를 복사합니다.

동일한 계정(동일한 파티션에 있든 동일한 AWS 리전 AWS 리전 파티션에 있든)의 AWS 스토리지 서비스 간에 전송할 때는 에이전트가 필요하지 않습니다. 데이터는 AWS 네트워크에 남아 있으며 퍼블릭 인터넷을 통과하지 않습니다.

> **Important**
>
> 사이에 전송된 데이터에 대해 비용을 지불합니다 AWS 리전. 이는 사용자 소스 리전에서 대상 리전으로 전송된 데이터에 대한 청구입니다. 자세한 내용은 데이터 전송 요금을 참조하십시오.

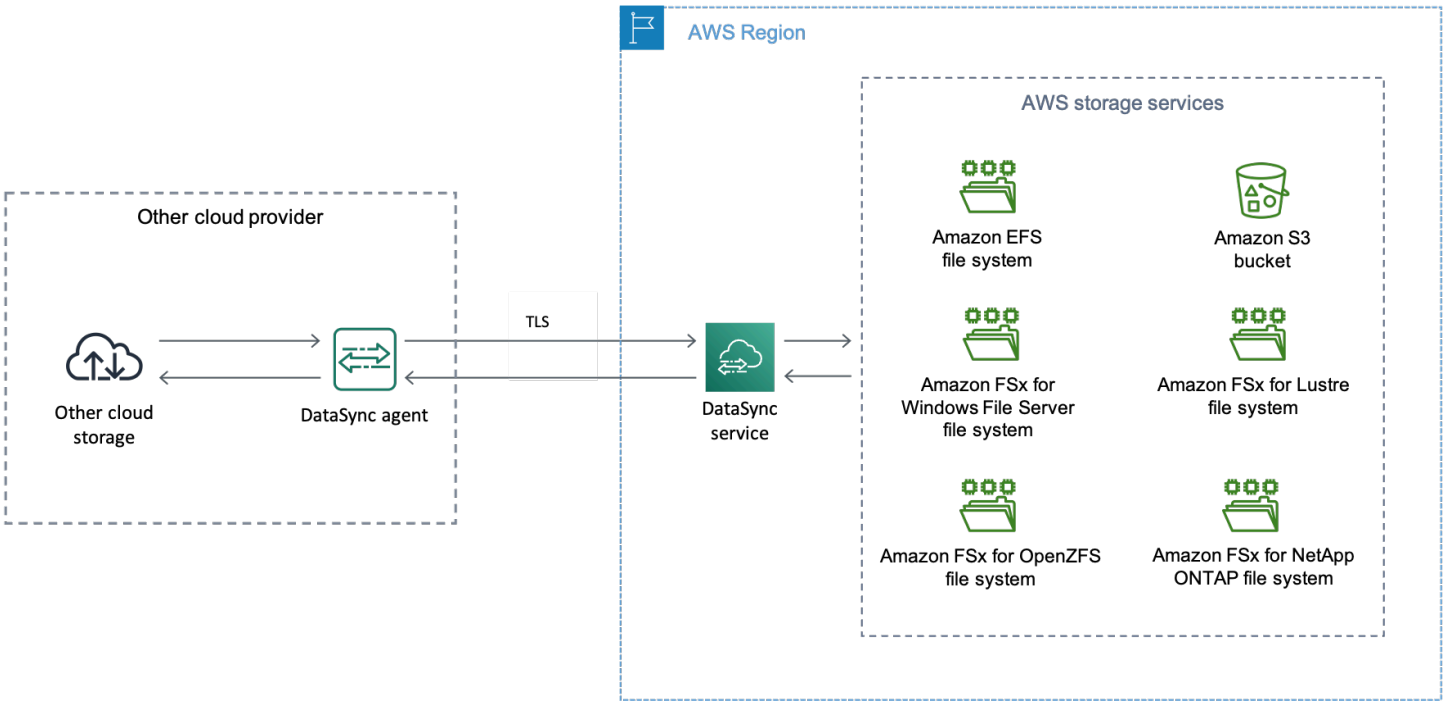
AWS 스토리지 서비스와 다른 클라우드의 스토리지 시스템 간 전송

DataSync를 사용하면 다른 클라우드 스토리지 시스템과 AWS 서비스사이에 데이터를 전송할 수 있습니다. 이러한 맥락에서 클라우드 스토리지 시스템에는 다음 스토리지가 포함될 수 있습니다.

- AWS내 가상 프라이빗 클라우드(VPC)의 NFS 파일 서버와 같은 자체 관리형 스토리지 시스템입니다.
- 다른 클라우드 공급자가 호스팅하는 스토리지 시스템 또는 서비스 자세한 내용은 를 사용하여 다른 클라우드 스토리지로 또는 다른 클라우드 스토리지에서 전송 AWS DataSync 단원을 참조하십시오.

DataSync는 에이전트를 사용하거나 사용하지 않고 다른 클라우드로 또는 다른 클라우드에서 데이터를 복사할 수 있습니다. 에이전트 사용 시기에 대한 자세한 내용은 AWS DataSync 에이전트가 필요한가요?를 참조하세요.

다음 다이어그램은 AWS 스토리지 서비스와 다른 클라우드 공급자 간에 데이터를 전송하는 DataSync에 대한 개략적인 개요를 보여줍니다.



개념 및 용어

DataSync 전송 기능을 숙지하세요.

주제

- 에이전트
- Location
- Task
- 작업 실행

에이전트

에이전트는 DataSync가 전송 중에 스토리지에서 읽고 쓰는 데 사용하는 가상 머신(VM) 어플라이언스입니다. DataSync는 두 가지 유형의 에이전트를 제공합니다. 하나는 기본 모드 작업을 처리하고 다른 하나는 향상된 모드 작업을 처리합니다. 사용 사례에 맞는 에이전트 선택에 대한 자세한 내용은 섹션을 참조하세요작업 모드에 대한 에이전트 선택.

VMware ESXi, Linux 커널 기반 가상 머신(KVM), Nutanix AHV(KVM 에이전트 이미지 사용) 또는 Microsoft Hyper-V 하이퍼바이저의 스토리지 환경에 에이전트를 배포할 수 있습니다. 의 Virtual Private Cloud(VPC)에 저장하는 AWS경우 에이전트를 Amazon EC2 인스턴스로 배포할 수 있습니다.

시작하려면 AWS DataSync 에이전트가 필요합니까?를 참조하십시오

Location

위치는 데이터를 복사해서 보내거나 복사해 오는 위치를 뜻합니다. 각 DataSync 전송(작업이라고도 함) 에는 소스 및 대상 위치가 있습니다. 자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.

Task

작업은 DataSync 전송을 뜻합니다. 소스 및 대상 위치와 해당 위치 사이에서 데이터를 복사하는 방법에 대한 세부 정보를 식별합니다. 또한 작업에서 메타데이터, 삭제된 파일, 권한을 처리하는 방법을 지정할 수 있습니다.

작업 실행

작업 실행은 DataSync 전송 작업의 개별 실행입니다. 작업 실행에는 여러 단계가 포함됩니다. 자세한 내용은 태스크 실행 상태 단원을 참조하십시오.

DataSync가 파일, 객체, 디렉터리를 전송하는 방법

DataSync는 작업 실행 중에 데이터를 준비, 전송, 확인합니다. DataSync가 이러한 작업을 수행하는 방법은 작업 모드와 같은 DataSync 작업 옵션을 구성하는 방법에 따라 달라집니다. 기본 모드 작업은 데이터를 순차적으로 준비, 전송, 확인하는 반면, 확장 모드 작업은 이러한 작업을 병렬로 수행합니다.

주제

- DataSync가 데이터 전송을 준비하는 방법
- DataSync가 데이터를 전송하는 방법
- DataSync가 데이터 무결성을 확인하는 방법
- DataSync가 열린 파일 및 잠긴 파일을 처리하는 방법
- 반복 전송 옵션

DataSync가 데이터 전송을 준비하는 방법

DataSync는 기본적으로 소스 및 대상 위치를 검사하여 전송할 데이터를 파악하고 전송을 준비합니다. 이는 두 위치의 콘텐츠와 메타데이터를 스캔하여 둘 사이의 차이를 식별함으로써 수행합니다.

> **Note**
>
> 모든 데이터를 전송하도록 작업을 구성하면 별도의 준비 단계를 거치지 않습니다. 작업을 시작하면 DataSync는 위치를 비교하지 않고 소스의 모든 데이터를 대상으로 즉시 전송합니다.

DataSync가 전송을 준비하는 방법도 작업 모드에 따라 달라집니다.

확장 모드 준비	기본 모드 준비
DataSync는 소스 위치에서 객체가 발견되는 대로 준비합니다. 준비는 소스에 객체가 더 나열되지 않을 때까지 작업 실행 내내 계속됩니다. 기본 모드와 달리 DataSync는 각 작업 실행 시 사실상 무제한의 객체를 준비할 수 있습니다.	준비는 소스 및 대상 위치의 파일, 객체, 디렉터리의 수와 스토리지 성능에 따라 몇 분에서 몇 시간, 또는 그 이상이 걸릴 수 있습니다. DataSync의 소스 및 대상 인벤토리에 포함된 항목은 작업 할당량에 포함됩니다. 할당량은 DataSync가 각 작업 실행 중에 전송하는 항목 수를 기반으로 하지 않습니다.

DataSync는 준비 중에 일부 파일, 객체, 디렉터리를 건너뛸 수 있습니다. 그 이유는 작업 구성 방법 및 스토리지 시스템 권한 등 여러 요인에 따라 달라질 수 있습니다. 여기 몇 가지 예가 있습니다:

- 소스 위치 및 대상 위치의 파일이 이미 있습니다. 소스의 파일은 이전 작업 실행 이후 수정되지 않았습니다. DataSync는 변경된 데이터만 전송하므로 다음 번에 작업을 실행할 때 해당 파일을 전송하지 않습니다.
- 두 위치에 모두 존재하는 객체가 소스에서 변경됩니다. 태스크가 대상의 데이터를 덮어쓰지 않기 때문에 태스크를 실행하면 DataSync는 대상에서 이 객체를 건너뜁니다.
- DataSync는 아카이브 스토리지 클래스를 사용 중이며 복원되지 않은 소스 위치의 객체를 건너뜁니다. DataSync가 읽을 수 있도록 아카이브된 객체를 복원해야 합니다.
- DataSync가 소스 위치에서 파일, 객체, 디렉터리를 읽을 수 없으므로 이를 건너뜁니다. 이런 일이 예상치 못하게 발생한 경우, 스토리지의 액세스 권한을 확인하고 DataSync가 건너뛴 항목을 읽을 수 있는지 확인하세요.

DataSync가 데이터를 전송하는 방법

DataSync는 작업 옵션에 따라 소스에서 대상으로 데이터(메타데이터 포함)를 복사합니다. 예를 들어, 복사할 메타데이터를 지정하고, 특정 파일을 제외하고, DataSync가 사용하는 대역폭의 양을 제한하는 등 다양한 옵션을 이용할 수 있습니다.

DataSync가 데이터를 전송하는 방법 또한 작업 모드에 따라 달라집니다.

확장 모드 전송	기본 모드 전송
DataSync는 각 객체가 준비되는 즉시 전송합니다.	DataSync가 모든 데이터를 준비하면 전송이 시작됩니다.

DataSync는 전송 중에 일부 항목을 건너뛸 수 있습니다. 모든 데이터를 전송하도록 작업을 구성하는 경우, 소스 위치에서 아카이브 스토리지 클래스를 사용 중이며 복원되지 않은 객체에 해당 문제가 발생할 수 있습니다.

DataSync가 데이터 무결성을 확인하는 방법

DataSync는 전송 중에 항상 데이터 무결성 검사를 수행합니다. 전송이 끝나면 DataSync는 전송된 데이터만 추가로 검사하거나 두 위치의 전체 데이터세트에 대해 추가로 검사할 수 있습니다. 자세한 내용은 가 데이터 무결성을 AWS DataSync 확인하는 방법 구성 단원을 참조하십시오.

데이터 무결성을 확인할 때 DataSync는 위치에 있는 파일, 객체, 디렉터리의 체크섬과 메타데이터를 계산하여 비교합니다. DataSync가 위치 간 차이를 발견하면 확인에 실패했다는 오류가 발생합니다. 예를 들면 `Checksum failure`, `Metadata failure`, `Files were added`, `Files were removed` 등의 오류가 표시될 수 있습니다.

확인 방식은 전송 종료 시 DataSync가 데이터 무결성을 확인하도록 구성했는지 여부와 작업 모드에 따라 달라집니다.

확장 모드 확인	기본 모드 확인
DataSync는 대상에 전송하는 각 객체를 확인합니다. 확장 모드에서 DataSync는 전송된 데이터만 확인합니다.	전송이 끝나면 DataSync가 데이터의 무결성을 확인합니다. 데이터 검증을 구성한 방식에 따라, 대규모 데이터세트에 대해 이 작업에 상당한 시간이 걸릴 수 있습니다.

DataSync가 열린 파일 및 잠긴 파일을 처리하는 방법

열린(사용 중) 파일이나 잠긴 파일을 전송하려고 할 때 다음 사항에 유의하세요.

- 일반적으로 DataSync는 열린 파일을 제한 없이 전송할 수 있습니다.
- 파일이 열려 있고 전송 중에 이 파일에 쓰고 있으면 DataSync가 전송 작업의 검증 과정 중에 데이터 불일치를 감지합니다. 최신 버전의 파일을 얻으려면 작업을 다시 실행해야 합니다.
- 파일이 잠겨 있고 서버가 DataSync의 파일 오픈을 막으면 DataSync는 전송 중에 파일을 건너뛰고 오류를 기록합니다.
- DataSync는 파일을 잠그거나 잠금 해제할 수 없습니다.

반복 전송 옵션

일회성 전송 외에도, DataSync는 데이터를 반복적으로 전송할 수 있습니다. 이러한 상황에 대한 몇 가지 옵션은 다음과 같습니다.

- 작업이 실행될 때 예약합니다.
- 이전 작업 실행 이후 변경된 데이터만 전송합니다.
- 소스에 더 이상 없는 대상 위치의 데이터를 삭제합니다.

시작하기 AWS DataSync

를 시작하기 전에가 없는 AWS 계정 경우에 가입 AWS DataSync해야 합니다. 또한 DataSync를 사용할 수 있는 위치와 데이터를 전송하는 데 드는 비용을 알아보는 것이 좋습니다.

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 확인하고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 그룹 추가를 참조하세요.

DataSync 사용 시 필요한 IAM 권한

DataSync는 Amazon S3 버킷, Amazon EFS 파일 시스템 또는 Amazon FSx 파일 시스템과 데이터를 주고받을 수 있습니다. 데이터를 원하는 곳으로 이동하려면 자격 증명에 올바른 IAM 권한을 부여해야 합니다. 예를 들어, DataSync와 함께 사용하는 IAM 역할에는 데이터를 S3 버킷으로 전송하는 데 필요한 Amazon S3 작업을 사용할 수 있는 권한이 필요합니다.

에서 제공하는 IAM 정책을 사용하거나 자체 정책을 생성 AWS 하여 이러한 권한을 부여할 수 있습니다.

목차

- AWS 관리형 정책
- 고객 관리형 정책

AWS 관리형 정책

AWS 는 일반적인 DataSync 사용 사례에 대해 다음과 같은 관리형 정책을 제공합니다.

- `AWSDataSyncReadOnlyAccess` - DataSync에 대한 읽기 전용 액세스 권한을 제공합니다.
- `AWSDataSyncFullAccess` - DataSync에 대한 전체 액세스 권한을 제공하며 그 종속성에 대한 최소한의 액세스 권한을 제공합니다.

자세한 설명은 AWS 에 대한 관리형 정책 AWS DataSync섹션을 참조하세요.

고객 관리형 정책

사용자 정의 IAM 정책을 생성하여 DataSync와 함께 사용할 수 있습니다. 자세한 내용은 에 대한 IAM 고객 관리형 정책 AWS DataSync 단원을 참조하십시오.

DataSync는 어디에 사용할 수 있나요?

DataSync가 지원하는 AWS 리전 및 엔드포인트 목록은의 AWS DataSync 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.

DataSync를 어떻게 사용할 수 있나요?

DataSync를 사용하는 몇 가지 방법은 다음과 같습니다.

- 의 일부인 DataSync 콘솔. AWS Management Console
- DataSync API 또는 AWS CLI를 사용하여 프로그래밍 방식으로 DataSync 구성 및 관리.
- AWS CloudFormation또는 Terraform을 사용하여 DataSync 리소스 제공
- DataSync를 사용하는 애플리케이션을 빌드하는 AWS SDKs.

DataSync의 비용은 얼마일까요?

전송하려는 데이터의 양을 사용하여 사용자 지정 견적을 생성하려면 DataSync 요금을 참조하세요.

DataSync가 사용하는 오픈 소스 구성 요소

DataSync에서 사용하는 오픈 소스 구성 요소를 보려면 다음 링크를 다운로드하세요.

- datasync-open-source-components.zip

AWS DataSync 에이전트가 필요합니까?

를 사용하려면 에이전트가 필요할 AWS DataSync수 있습니다. 에이전트는 데이터 전송을 위해 스토리지 환경에 배포하는 가상 머신(VM) 어플라이언스입니다.

에이전트가 필요한지 여부는 송수신하는 스토리지 유형, 송수신하는 스토리지 유형 AWS 계정, 송수신하는 스토리지 등 여러 요인 AWS 리전 에 따라 달라집니다. 자세한 내용을 읽기 전에 관심이 있는 전송을 DataSync가 지원하는지 확인하세요.

DataSync가 전송 시나리오를 지원하는지 확인한 후 다음 정보를 검토하면 에이전트가 필요한지 파악하는 데 도움이 됩니다.

DataSync 에이전트가 필요한 상황

DataSync 에이전트가 필요한 대부분의 상황에는 사용자 또는 다른 클라우드 공급자가 관리하는 스토리지가 포함됩니다.

- AWS 스토리지 서비스와 온프레미스 스토리지 간 전송
- Amazon EFS 또는 Amazon FSx와 다른 클라우드의 스토리지 간 전송
- 에서 AWS 계정 일부 AWS 스토리지 서비스 간 전송(스토리지 서비스가 Amazon S3가 아닌 경우)
- AWS GovCloud (US) Region 소스 AWS 리전 와 대상이 Amazon EFS 또는 Amazon FSx인 상용 및 간 전송

DataSync 에이전트가 필요하지 않은 상황

에이전트가 필요하지 않은 상황은 동일한 AWS 리전에서 또는 리전 간에 전송하든 관계없이 적용됩니다.

- 동일한의 AWS 스토리지 서비스 간 전송 AWS 계정
- 에서 Amazon S3와 다른 AWS 스토리지 서비스 간 전송 AWS 계정
- Amazon S3와 다른 클라우드의 객체 스토리지 간 전송
- AWS GovCloud (US) 소스 또는 대상이 Amazon S3인 상용 AWS 리전 와 간에 전송

작업 모드에 대한 에이전트 선택

DataSync 작업은 기본 모드 또는 향상된 모드에서 실행됩니다. 기본 모드 작업에는 기본 모드 에이전트가 필요합니다. 향상된 모드 작업에는 향상된 모드 에이전트가 필요합니다.

기본 모드는 다음 위치에 복사하거나 다음 위치에서 복사할 때 에이전트 사용을 지원합니다.

- NFS
- SMB
- HDFS
- 객체 스토리지(기타 클라우드 포함)
- Azure Blob

향상된 모드는 다음 위치에서 Amazon S3와의 전송을 위해 에이전트 사용을 지원합니다.

- NFS
- SMB

자세한 내용은 데이터 전송을 위한 작업 모드 선택 단원을 참조하십시오.

여러 DataSync 에이전트 사용

대부분 전송은 하나의 에이전트만 필요하지만 여러 에이전트를 사용하면 수백만 개의 파일 또는 객체가 포함된 대규모 데이터세트를 빠르게 전송할 수 있습니다. 이러한 상황에서는 작업당 하나의 에이전트를 사용하여 전송 작업을 병렬로 실행하는 것이 좋습니다. 이 접근 방식은 전송 워크로드를 여러 작업으로 분산하며, 각 작업은 자체 에이전트를 사용합니다. 또한 DataSync가 데이터를 준비하고 전송하는 데 걸리는 시간을 줄이는 데도 도움이 됩니다. 자세한 내용은 여러 작업으로 대규모 데이터세트 파티셔닝 단원을 참조하십시오.

또 다른 옵션은 특히 수백만 개의 작은 파일이 있는 경우, 전송 위치에 여러 에이전트를 사용하는 것입니다. 예를 들어 온프레미스 네트워크 파일 시스템(NFS) 파일 서비스에 최대 4개의 에이전트를 연결할

수 있습니다. 이 옵션을 사용하면 전송 속도를 높일 수 있지만, DataSync가 전송을 준비하는 데 걸리는 시간은 변하지 않습니다.

둘 중 어느 방법을 사용하든 스토리지의 I/O 작업이 증가하고 네트워크 대역폭에 영향을 미칠 수 있다는 점에 유의하세요. DataSync 전송에 여러 에이전트를 사용하는 방법에 대한 자세한 내용은 AWS 스토리지 블로그를 참조하십시오.

여러 에이전트를 사용하려는 경우 다음을 기억해야 합니다.

- 위치에는 최대 4개의 기본 모드 에이전트와 최대 4개의 향상된 모드 에이전트가 할당될 수 있습니다. 위치를 사용하는 작업은 구성된 작업 모드에 해당하는 에이전트만 사용합니다.
- 한 위치에 에이전트를 여러 명 사용한다고 해서 가용성이 높아지지는 않습니다. 특정 위치에 연결된 모든 에이전트가 온라인 상태여야 전송 작업을 시작할 수 있습니다. 에이전트 중 하나가 오프라인 상태인 경우 작업을 실행할 수 없습니다.
- 가상 프라이빗 클라우드(VPC) 서비스 엔드포인트를 사용하여 DataSync 서비스와 통신하려면 모든 에이전트가 동일한 엔드포인트와 서브넷을 사용해야 합니다.

다음 단계

- 에이전트가 필요한 경우 에이전트 요구 사항을 검토하여 스토리지 환경에 적합한지 여부를 파악합니다.
- 전송에 에이전트가 필요하지 않은 경우 전송 구성을 시작할 수 있습니다.

AWS DataSync 에이전트에 대한 요구 사항

스토리지 환경에 AWS DataSync 에이전트를 배포하기 전에 에이전트 하이퍼바이저 및 리소스 요구 사항을 이해해야 합니다.

하이퍼바이저 요구 사항

지원되는 하이퍼바이저에 DataSync 에이전트를 배포하여 데이터 전송을 용이하게 할 수 있습니다.

> **Note**
>
> 향상된 모드 에이전트는 VMware ESXi, KVM, Nutanix AHV 및 만 지원합니다EC2.

다음 하이퍼바이저에서 DataSync 에이전트를 실행할 수 있습니다.

- VMware ESXi(버전 7.0 또는 8.0): VMware ESXi는 Broadcom 웹 사이트에서 사용할 수 있습니다. 호스트에 접속하려면 VMware vSphere 클라이언트도 필요합니다.
- Linux 커널 기반 가상 머신(KVM): 무료 오픈 소스 가상화 기술입니다. KVM은 Linux 버전 2.6.20 이상에 포함되어 있습니다. DataSync는 Centos/RHEL 7 및 8, Ubuntu 16.04 LTS 및 Ubuntu 18.04 LTS 배포판에 대해 테스트되고 지원됩니다. 다른 최신 Linux 배포판이 작동할 수 있지만 기능이나 성능이 보장되지는 않습니다. DataSync 에이전트를 배포하려면 KVM 호스트에서 하드웨어 가속화 가상화를 활성화해야 합니다.

  KVM 환경이 이미 가동되고 있고 KVM 작동 방식에 익숙하다면 이 옵션을 사용하는 것이 좋습니다.

  Amazon EC2에서는 KVM을 실행할 수 없으며 DataSync 에이전트에 사용할 수 없습니다.
- Microsoft Hyper-V(버전 2012 R2, 2016 또는 2019): 기본 모드 에이전트만 해당. 이 설정의 경우 호스트에 연결하려면 Microsoft Windows 클라이언트 컴퓨터에서 Microsoft Hyper-V Manager를 사용해야 합니다.

  DataSync 에이전트는 1세대 가상 머신(VM)입니다. 1세대 VM과 2세대 VM 간의 차이점에 대한 자세한 내용은 Hyper-V에서 1세대 또는 2세대 가상 컴퓨터를 만들어야 합니까?를 참조하세요.
- Amazon EC2: DataSync는 DataSync 이미지를 포함하는 Amazon Machine Image(AMI)를 제공합니다. 권장 인스턴스 유형은 Amazon EC2 인스턴스 요구 사항 단원을 참조하십시오.

DataSync 전송을 위한 에이전트 요구 사항

DataSync 전송의 경우 에이전트는 다음 리소스 요구 사항을 충족해야 합니다.

> **Important**
>
> 최대 2천만 개의 파일, 객체 또는 디렉터리 작업에 대한 기본 모드 에이전트 요구 사항은 일반적인 지침입니다. 보유한 디렉터리 수, 개체 메타데이터 크기 등 다른 요인으로 인해 에이전트에 더 많은 리소스가 필요할 수 있습니다. 예를 들어, Amazon EC2 에이전트용 m5.2xlarge 인스턴스로는 2천만 개 미만의 파일을 전송하기에 여전히 충분하지 않을 수 있습니다.
> 향상된 모드 에이전트에는 파일 할당량이 없습니다.

목차

- 가상 머신 요구 사항
- Amazon EC2 인스턴스 요구 사항

가상 머신 요구 사항

Amazon EC2 인스턴스에 없는 DataSync 에이전트를 배포할 때 에이전트 VM에는 기본 모드 에이전트를 사용하는지 아니면 향상된 모드 에이전트를 사용하는지에 따라 다음 리소스가 필요합니다.

Resource	기본 모드	확장 모드
가상 프로세서	VM에 지정한 가상 프로세스 4개	VM에 할당된 가상 프로세서 8개
디스크 공간	VM 이미지 및 시스템 데이터를 설치하기 위한 80GB의 디스크 공간	VM 이미지 및 시스템 데이터를 설치하기 위한 80GB의 디스크 공간
RAM	최대 2천만 개의 파일, 객체 또는 디렉터리로 작업 실행을 위해 VM에 할당된 32GB의 RAM 2천만 개 이상의 파일, 객체 또는 디렉터리로 작업 실행을 위해 VM에 할당된 64GB의 RAM	VM에 할당된 32GB RAM

Amazon EC2 인스턴스 요구 사항

Amazon EC2 인스턴스에 DataSync 에이전트를 배포할 때는 인스턴스 크기가 2배 이상이어야 합니다. 기본 모드 에이전트를 사용하는지 아니면 향상된 모드 에이전트를 사용하는지에 따라 다음 인스턴스 크기 중 하나를 사용하는 것이 좋습니다.

기본 모드 에이전트	향상된 모드 에이전트
최대 2천만 개의 파일, 객체 또는 디렉터리로 작업하는 태스크 실행의 경우 m5.2xlarge를 사용합니다. 2천만 개 이상의 파일, 객체 또는 디렉터리로 작업하는 태스크 실행의 경우 m5.4xlarge를 사용합니다.	데이터 세트의 파일, 객체 또는 디렉터리 수에 관계없이 m6a.2xlarge를 사용합니다.

AWS 리전 파티션에 대한 에이전트 요구 사항

DataSync 에이전트 이미지는 특정 AWS 리전 파티션과 연결되어 있습니다. 예를 들어 기본적으로 상용에서 에이전트를 다운로드 AWS 리전 한 다음에서 활성화할 수 없습니다 AWS GovCloud (US) Region.

에이전트 관리 요구 사항

DataSync 에이전트를 활성화하면 AWS 가 자동으로 에이전트를 관리합니다. 자세한 내용은 AWS DataSync 에이전트 관리 단원을 참조하십시오.

AWS DataSync 에이전트 배포

AWS DataSync 에이전트를 생성할 때 첫 번째 단계는 스토리지 환경에 에이전트를 배포하는 것입니다. VMware ESXi, Linux 커널 기반 가상 머신(KVM), Nutanix AHV(KVM 이미지 사용) 및 Microsoft Hyper-V 하이퍼바이저에서 에이전트를 가상 머신(VM)으로 배포할 수 있습니다. 또한 AWS의 가상 프라이빗 클라우드(VPC)에 있는 Amazon EC2 인스턴스를 에이전트로 배포할 수 있습니다.

> **Tip**
>
> 시작하기 전에 DataSync 에이전트가 필요한지 확인합니다.

VMware에 에이전트 배포

DataSync 콘솔에서 에이전트를 다운로드하여 VMware 환경에 배포할 수 있습니다.

시작하기 전: 스토리지 환경이 DataSync 에이전트를 지원할 수 있는지 확인하세요. 자세한 설명은 가상 머신 요구 사항섹션을 참조하세요.

VMware에 에이전트를 배포하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택한 다음, 에이전트 생성을 선택합니다.
3. 하이퍼바이저에서 VMware ESXi를 선택한 다음 이미지 다운로드를 선택합니다.
   - 향상된 모드 에이전트는 `.ova` 이미지 파일로 다운로드됩니다.

- 기본 모드 에이전트는 `.ova` 이미지 `.zip` 파일이 포함된 파일로 다운로드합니다.

4. 네트워크 지연 시간을 최소화하려면 DataSync가 액세스해야 하는 스토리지 시스템(가능한 경우 동일한 로컬 네트워크) 에 에이전트를 최대한 가깝게 배포하세요. 자세한 내용은 온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항 단원을 참조하십시오.

   필요한 경우 VMware 호스트에 `.ova`파일을 배포하는 방법에 대한 하이퍼바이저 설명서를 참조하세요.

5. 하이퍼바이저의 전원을 켜고 에이전트 VM에 로그인한 다음, 에이전트의 IP 주소를 가져옵니다. 에이전트를 활성화하려면 이 IP 주소가 필요합니다.

   에이전트 VM의 기본 보안 인증은 로그인 **admin**및 암호 **password**입니다. 필요한 경우 VM의로컬 콘솔을 통해 비밀번호를 변경하세요.

다음 단계: AWS DataSync 에이전트의 서비스 엔드포인트 선택

KVM에 에이전트 배포

DataSync 콘솔에서 에이전트를 다운로드하고 KVM 환경에 배포할 수 있습니다.

시작하기 전: 스토리지 환경이 DataSync 에이전트를 지원할 수 있는지 확인하세요. 자세한 설명은 가상 머신 요구 사항섹션을 참조하세요.

KVM에 에이전트를 배포하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택한 다음, 에이전트 생성을 선택합니다.
3. 하이퍼바이저에서 커널 기반 가상 머신(KVM) 을 선택한 다음 이미지 다운로드를 선택합니다.

   - 향상된 모드 에이전트는 `.qcow2` 이미지 파일로 다운로드됩니다.
   - 기본 모드 에이전트는 `.qcow2` 이미지 `.zip` 파일이 포함된 파일로 다운로드합니다.

4. 네트워크 지연 시간을 최소화하려면 DataSync가 액세스해야 하는 스토리지 시스템(가능한 경우 동일한 로컬 네트워크) 에 에이전트를 최대한 가깝게 배포하세요. 자세한 내용은 온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항 단원을 참조하십시오.
5. 다음 명령을 실행하여 `.qcow2`이미지를 설치합니다.

```
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
```

이 VM과 KVM 호스트를 관리하는 방법에 대한 자세한 내용은 하이퍼바이저 설명서를 참조하세요.

6. 하이퍼바이저의 전원을 켜고 VM에 로그인한 다음, 에이전트의 IP 주소를 가져옵니다. 에이전트를 활성화하려면 이 IP 주소가 필요합니다.

   에이전트 VM의 기본 보안 인증은 로그인 **admin**및 암호 **password**입니다. 필요한 경우 VM의로컬 콘솔을 통해 비밀번호를 변경하세요.

다음 단계: AWS DataSync 에이전트의 서비스 엔드포인트 선택

Microsoft Hyper-V에 기본 모드 에이전트 배포

DataSync 콘솔에서 기본 모드 에이전트를 다운로드하여 Microsoft Hyper-V 환경에 배포할 수 있습니다.

시작하기 전: 스토리지 환경이 DataSync 에이전트를 지원할 수 있는지 확인하세요. 자세한 내용은 가상 머신 요구 사항 단원을 참조하십시오.

Hyper-V에 기본 모드 에이전트를 배포하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택한 다음, 에이전트 생성을 선택합니다.
3. 하이퍼바이저의에서 Microsoft Hyper-V를 선택한 다음 이미지 다운로드를 선택합니다.

   에이전트는 이미지 `.vhdx`파일이 포함된 `.zip`파일로 다운로드합니다.
4. 네트워크 지연 시간을 최소화하려면 DataSync가 액세스해야 하는 스토리지 시스템(가능한 경우 동일한 로컬 네트워크) 에 에이전트를 최대한 가깝게 배포하세요. 자세한 내용은 온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항 단원을 참조하십시오.

   필요한 경우 Hyper-V 호스트에 `.vhdx`파일을 배포하는 방법에 대한 하이퍼바이저 설명서를 참조하세요.

> **Warning**
>
> Broadcom 네트워크 어댑터를 사용하는 Hyper-V 호스트에서 가상 컴퓨터 대기열(VMQ)을 사용하도록 설정하면 네트워크 성능이 저하될 수 있습니다. 해결 방법에 대한 자세한 정보는 Microsoft 설명서를 참조하십시오.

5. 하이퍼바이저의 전원을 켜고 VM에 로그인한 다음, 에이전트의 IP 주소를 가져옵니다. 에이전트를 활성화하려면 이 IP 주소가 필요합니다.

   에이전트 VM의 기본 보안 인증은 로그인 **admin**및 암호 **password**입니다. 필요한 경우 VM의로컬 콘솔을 통해 비밀번호를 변경하세요.

다음 단계: AWS DataSync 에이전트의 서비스 엔드포인트 선택

Amazon EC2 에이전트 배포

다음 간에 데이터를 전송할 때 DataSync 에이전트를 Amazon EC2 인스턴스로 배포할 수 있습니다.

- 자체 관리형 클라우드 스토리지 시스템(예:의 NFS 파일 서버 AWS) 및 AWS 스토리지 서비스.
- 클라우드 스토리지 공급자(예: Microsoft Azure Blob Storage 또는 Google Cloud Storage) 및 기본 모드를 사용하는 AWS 스토리지 서비스.
- 상용의 S3 버킷 AWS 리전 과의 S3 버킷. AWS GovCloud (US) Region
- 기본 모드를 사용하는 Amazon S3 on AWS Outposts 및 AWS 스토리지 서비스.

> **Warning**
>
> 네트워크 지연 시간이 길어지기 때문에 온프레미스 스토리지와 함께 Amazon EC2 에이전트를 사용하지 않는 것이 좋습니다. 대신 에이전트를 온프레미스 스토리지와 최대한 가까운 데이터 센터에 VMware, KVM 또는 Hyper-V 가상 머신으로 배포하세요.

EC2 에이전트 배포

에 대한 에이전트 AMI를 선택하려면 AWS 리전

1. 터미널을 열고 다음 AWS CLI 명령을 복사하여 Amazon EC2 에이전트를 배포하려는 리전의 최신 DataSync Amazon Machine Image(AMI) ID를 가져옵니다.

   기본 모드 에이전트

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

   향상된 모드 에이전트

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

2. 명령을 실행합니다. 출력에서 DataSync AMI ID로 "Value" 속성을 기록해 둡니다.

   Example예제 명령 및 출력

   ```
   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"
       }
   }
   ```

Amazon EC2 에이전트를 배포하려면

> **Tip**
>
> 가용 영역 간 전송에 대해 요금이 부과되지 않게 하려면 가용 영역 간 네트워크 트래픽이 필요하지 않은 방식으로 에이전트를 배포합니다. (모든의 데이터 전송 요금에 대한 자세한 내용은 Amazon EC2 데이터 전송 요금을 AWS 리전참조하세요.)
> 예를 들어 자체 관리형 클라우드 스토리지 시스템이 있는 가용 영역에 에이전트를 배포합니다.

1. 다음 URL을 복사합니다.

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

- *agent-region*를 에이전트를 배포할 리전으로 바꿉니다.
- *ami-id*를 가져온 DataSync AMI ID로 바꿉니다.

2. 브라우저에 URL을 붙여 넣습니다.

   의 Amazon EC2 인스턴스 시작 페이지가 AWS Management Console 표시됩니다.
3. 인스턴스 유형에서 DataSync용 권장 Amazon EC2 인스턴스 중 하나를 선택합니다.
4. 키 페어 이름에서 기존 키 페어를 선택하거나 새 이름을 생성합니다.
5. 네트워크 설정에서 편집을 선택하고 다음을 수행합니다.

   a. VPC에서 에이전트를 배포하려는 VPC를 선택합니다.

   b. 퍼블릭 IP 자동 할당에서 퍼블릭 인터넷에서 에이전트에 액세스할 수 있도록 할지 여부를 선택합니다.

      나중에 인스턴스의 퍼블릭 또는 프라이빗 IP 주소를 사용하여 에이전트를 활성화합니다.

   c. 방화벽(보안 그룹)에서 다음을 수행하는 보안 그룹을 만들거나 선택하세요.

      - 필요한 경우 포트 80(HTTP)의 Amazon EC2 인스턴스에 대한 인바운드 트래픽을 허용합니다. 에이전트 활성화 키 가져오기의 일부 옵션에는 이 연결이 필요합니다.
      - Amazon EC2 인스턴스와 데이터를 전송하려는 스토리지 시스템 간의 인바운드 및 아웃바운드 트래픽을 허용합니다. 자세한 내용은 온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항 단원을 참조하십시오.

      > **Note**
      >
      > 에이전트가 사용하는 서비스 엔드포인트 유형에 따라 추가 포트를 구성해야 합니다.

6. (권장) 클라우드 기반 파일 시스템에서 전송 성능을 높이려면 고급 세부 정보를 펼치고 스토리지가 위치한 배치 그룹 값을 선택합니다.
7. Amazon EC2 인스턴스를 시작하려면 시작 인스턴스를 선택합니다.
8. 인스턴스 상태가 실행 중이면 인스턴스를 선택합니다.
9. 퍼블릭 인터넷에서 액세스할 수 있도록 인스턴스를 구성한 경우 인스턴스의 퍼블릭 IP 주소를 기록해 두세요. 그렇지 않은 경우 사설 IP 주소를 기록해 두세요.

에이전트를 활성화할 때 이 IP 주소가 필요합니다.

예:에 EC2 에이전트 배포 AWS 리전

다음 지침은 DataSync 에이전트를 AWS 리전에서 배포하는 경우 일반 시나리오에 도움이 될 수 있습니다.

주제

- 클라우드 스토리지와 AWS 스토리지 서비스 간 전송을 위한 기본 모드 에이전트 배포
- Amazon S3와 AWS 파일 시스템 간 전송을 위한 기본 모드 에이전트 배포

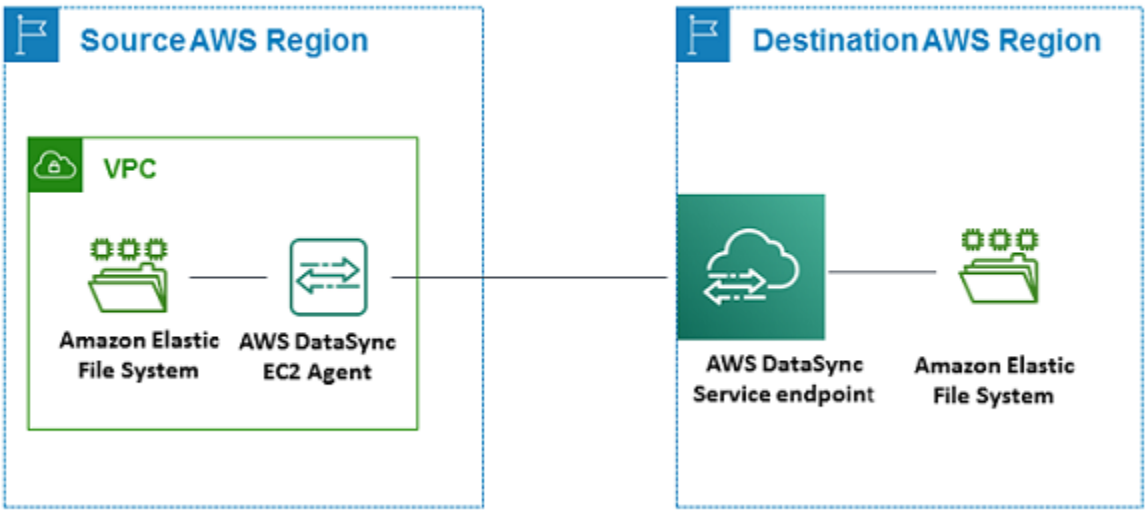
클라우드 스토리지와 AWS 스토리지 서비스 간 전송을 위한 기본 모드 에이전트 배포

클라우드 스토리지 시스템 간에 AWS 계정또는 클라우드 스토리지 시스템 간에 데이터를 전송하려면 DataSync 에이전트가 소스 파일 시스템이 있는 동일한 AWS 리전 및 AWS 계정 에 있어야 합니다. 이 유형의 전송에는 다음이 포함됩니다.

- Amazon EFS 또는 Amazon FSx 간에 다른의 AWS 스토리지로 전송합니다 AWS 계정.
- 자체 관리형 파일 시스템에서 AWS 스토리지 서비스로 전송합니다.

> **Important**
>
> 가용 영역 간 네트워크 트래픽이 필요하지 않도록 에이전트를 배포하세요(이러한 트래픽에 대한 요금 부과를 피하기 위한).
>
> - Amazon EFS 또는 FSx for Windows File Server 파일 시스템에 액세스하려면 파일 시스템에 탑재 대상이 있는 가용 영역에 에이전트를 배포하세요.
> - 자체 관리형 파일 시스템의 경우 파일 시스템이 있는 가용 영역에 에이전트를 배포하세요.
>
> 모든의 데이터 전송 요금에 대한 자세한 내용은 Amazon EC2 온디맨드 요금을 AWS 리전참조하세요.

예를 들어, 다음 다이어그램은 클라우드 내 네트워크 파일 시스템(NFS)에서 클라우드 내 NFS 또는 Amazon S3로 데이터를 전송하는 DataSync 아키텍처를 개괄적으로 보여줍니다.

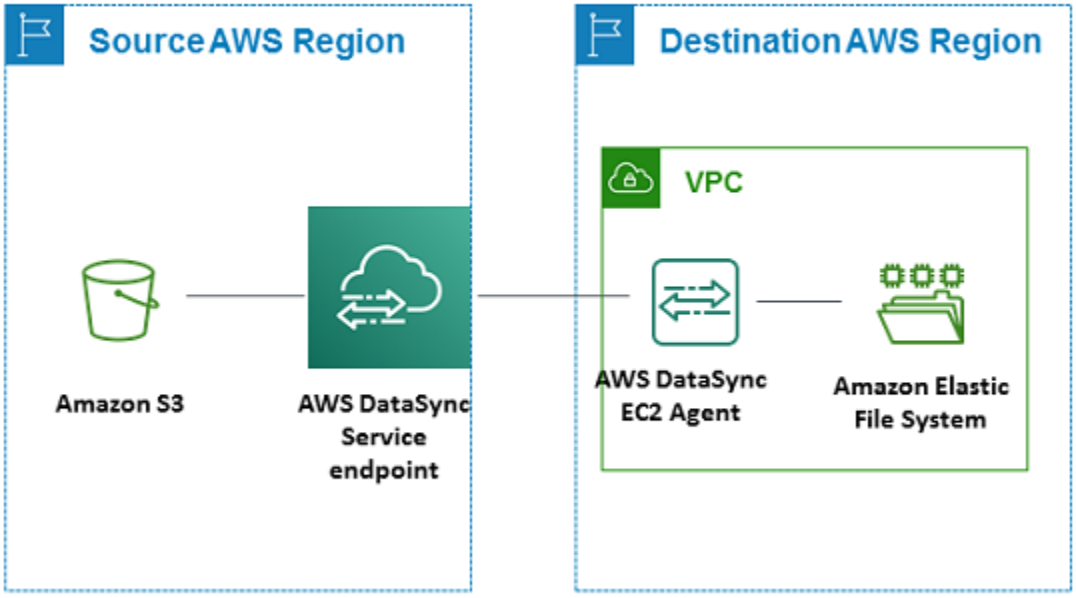


AWS 스토리지 서비스 간에 전송할 때는 AWS 계정다음 사항에 유의하십시오.

- NFS 프로토콜을 사용하여 Amazon EFS 파일 시스템 또는 Amazon FSx 파일 시스템 간에 전송할 때, 소스 파일 시스템을 NFS 위치로 구성합니다.
- SMB 프로토콜을 사용하여 Amazon FSx 파일 시스템 간에 전송할 때, 소스 파일 시스템을 SMB 위치로 구성합니다.

Amazon S3와 AWS 파일 시스템 간 전송을 위한 기본 모드 에이전트 배포

다음 다이어그램은 Amazon S3에서 Amazon EFS 또는 Amazon FSx와 같은 AWS 파일 시스템으로 데이터를 전송하기 위한 DataSync 아키텍처의 상위 수준 보기를 제공합니다. 이 아키텍처를 사용하여 데이터를 한에서 다른 AWS 계정 로 전송하거나 Amazon S3에서 자체 관리형 클라우드 내 파일 시스템으로 데이터를 전송할 수 있습니다.



에 기본 모드 에이전트 배포 AWS Outposts

사용자 Outpost에서 DataSync Amazon EC2 인스턴스를 시작할 수 있습니다. 에서 AMI를 시작하는 방법에 대한 자세한 내용은 AWS Outposts 사용 설명서의 Outpost에서 인스턴스 시작을 AWS Outposts 참조하세요. https://docs.aws.amazon.com/outposts/latest/userguide/launch-instance.html

DataSync를 사용하여 Amazon S3 on Outposts에 액세스하는 경우 기본 모드 에이전트를 사용하여 Amazon S3 액세스 포인트에 액세스할 수 있는 VPC에서 시작하고 Outpost의 상위 리전에서 에이전트를 활성화해야 합니다. 또한 에이전트는 해당 버킷의 Outposts 엔드포인트에서 Amazon S3로 라우팅할 수 있어야 합니다. Outposts 엔드포인트에서 Amazon S3를 사용하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 Outposts에서 Amazon S3 사용을 참조하세요.

AWS DataSync 에이전트의 서비스 엔드포인트 선택

서비스 엔드포인트는 AWS DataSync 에이전트가 DataSync 서비스와 통신하는 방법입니다. DataSync는 다음과 같은 유형의 서비스 엔드포인트를 지원합니다.

- 퍼블릭 서비스 엔드포인트-데이터는 퍼블릭 인터넷을 통해 전송됩니다.
- Federal Information Processing Standard(FIPS) 서비스 엔드포인트-FIPS를 준수하는 프로세스를 사용하여 공용 인터넷을 통해 데이터를 전송합니다.
- 가상 프라이빗 클라우드(VPC) 서비스 엔드포인트-공용 인터넷 대신 VPC를 통해 데이터가 전송되므로 전송된 데이터의 보안이 강화됩니다.

- FIPS VPC 서비스 엔드포인트 - 데이터는 FIPS를 준수하는 프로세스를 사용하여 VPC를 통해 전송됩니다.

에이전트를 활성화하기 위해 서비스 엔드포인트가 필요합니다. 서비스 엔드포인트를 선택할 때 다음 사항에 주의하세요.

- 에이전트는 한 가지 유형의 엔드포인트만 사용할 수 있습니다. 다른 엔드포인트 유형을 사용하여 데이터를 전송해야 하는 경우 유형별로 에이전트를 생성합니다.
- 스토리지 네트워크를 AWS에 연결하는 방법에 따라 사용할 수 있는 서비스 엔드포인트가 결정됩니다.

퍼블릭 서비스 엔드포인트 선택

퍼블릭 서비스 엔드포인트를 사용하면 DataSync 에이전트와 DataSync 서비스 간의 모든 통신은 퍼블릭 인터넷을 통해 이루어집니다.

1. 사용할 DataSync 퍼블릭 서비스 엔드포인트를 결정합니다.
2. DataSync 퍼블릭 서비스 엔드포인트를 사용하는 데 필요한 트래픽을 허용하도록 네트워크를 구성합니다.

다음 단계: AWS DataSync 에이전트 활성화

FIPS 서비스 엔드포인트 선택

DataSync는 FIPS를 준수하는 일부 서비스 엔드포인트를 제공합니다. 자세한 내용은 AWS 일반 참조의 FIPS 엔드포인트를 참조하세요.

1. 사용할 DataSync FIPS 서비스 엔드포인트를 결정합니다.
2. DataSync FIPS 서비스 엔드포인트를 사용하는 데 필요한 트래픽을 허용하도록 네트워크를 구성합니다.

다음 단계: AWS DataSync 에이전트 활성화

VPC 서비스 엔드포인트 선택

VPC 서비스 엔드포인트를 사용하는 경우 데이터는 퍼블릭 인터넷을 통해 전송되지 않습니다. 대신 DataSync는 Amazon VPC 서비스를 기반으로 하는 VPC를 통해 데이터를 전송합니다.

목차

- DataSync 에이전트가 VPC 서비스 엔드포인트와 작동하는 방식
- VPC 사용의 DataSync 제한
- DataSync에 대한 VPC 서비스 엔드포인트 생성

DataSync 에이전트가 VPC 서비스 엔드포인트와 작동하는 방식

VPC 서비스 엔드포인트는에서 제공합니다 AWS PrivateLink. 이러한 유형의 엔드포인트를 사용하면 지원되는를 VPC에 비공개 AWS 서비스 로 연결할 수 있습니다. DataSync와 함께 VPC 서비스 엔드포인트를 사용하는 경우 DataSync 에이전트와 DataSync 서비스 간의 모든 통신은 VPC에 남아 있습니다.

VPC 서비스 엔드포인트(DataSync가 데이터 전송 트래픽을 위해 생성하는 네트워크 인터페이스와 함께)는 VPC 내부에서만 액세스할 수 있는 프라이빗 IP 주소를 사용합니다. 자세한 내용은 AWS DataSync 전송을 위해 네트워크 연결 단원을 참조하십시오.

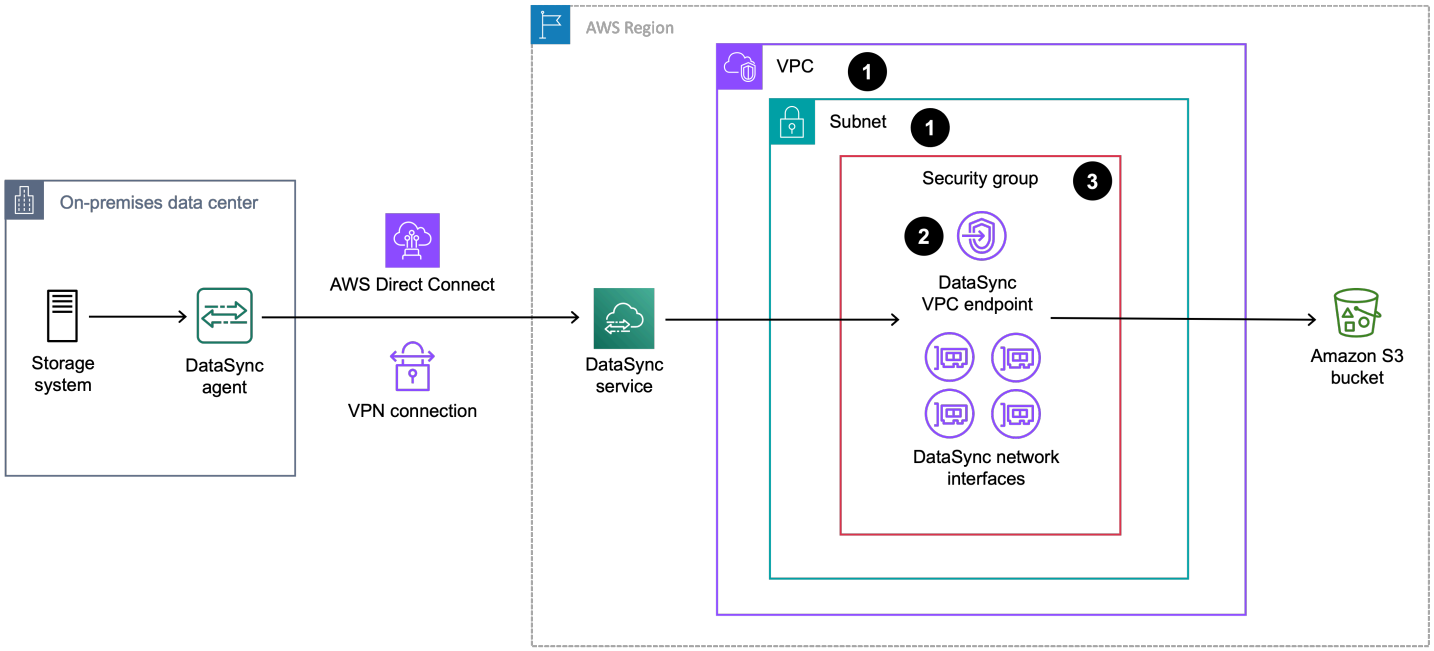
VPC 사용의 DataSync 제한

- DataSync와 함께 사용하는 VPC에는 기본 테넌시가 있어야 합니다. 전용 테넌시가 있는 VPC는 지원되지 않습니다.
- DataSync는 공유 VPC를 지원하지 않습니다.

DataSync에 대한 VPC 서비스 엔드포인트 생성

관리하는 VPC에서 DataSync에 대한 VPC 서비스 엔드포인트를 생성합니다. 서비스 엔드포인트, VPC, DataSync 에이전트는 동일한 AWS 계정에 속해야 합니다.

다음 다이어그램은 온프레미스 스토리지 시스템에서 Amazon S3 버킷으로 전송하기 위해 VPC 서비스 엔드포인트를 사용하는 DataSync의 예를 보여줍니다. 번호가 매겨진 콜아웃은 VPC 서비스 엔드포인트를 생성하는 단계에 해당합니다.



DataSync에 대한 VPC 서비스 엔드포인트를 생성하려면

1. VPC 서비스 엔드포인트를 생성할 VPC 및 서브넷을 생성하거나 결정합니다.

   외부에 있는 스토리지로 또는 스토리지에서 전송하는 경우 VPC AWS는 해당 스토리지 환경으로 확장해야 합니다(예: 스토리지 환경은 온프레미스 NFS 파일 서버가 위치한 데이터 센터일 수 있음). Direct Connect 또는 VPN을 통한 라우팅 규칙을 사용하여 이 작업을 수행할 수 있습니다.

2. 다음을 수행하여 DataSync VPC 서비스 엔드포인트를 생성합니다.

   a. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

   b. 왼쪽 탐색 창에서 엔드포인트를 선택하고 엔드포인트 생성을 선택합니다.

   c. 서비스 범주(Service category)에서 AWS 서비스를 선택합니다.

   d. 서비스에서 현재 AWS 리전 있는의 엔드포인트를 검색**datasync**하고 선택합니다(예: `com.amazonaws.us-east-1.datasync` 또는 `com.amazonaws.us-east-1.datasync-fips`).

   e. VPC에서 VPC 서비스 엔드포인트를 만들 VPC를 선택합니다.

   f. 추가 설정을 확장하고 프라이빗 DNS 이름 활성화 확인란을 선택 취소하여 이 설정을 비활성화합니다.

      동일한 VPC에 퍼블릭 서비스 엔드포인트를 사용해야 하는 에이전트가 있는 경우 이 설정을 비활성화하는 것이 좋습니다. 이 설정을 활성화하면 에이전트가 네트워크를 통해 퍼블릭 서비스 엔드포인트에 연결할 수 없습니다.

g. 서브넷에서 VPC 서비스 엔드포인트를 생성할 서브넷을 선택합니다. 서브넷 ARN을 기록해 둡니다(에이전트를 활성화할 때 필요).

h. 엔드포인트 생성을 선택합니다. 엔드포인트 ID를 기록해 둡니다(에이전트를 활성화할 때 필요).

3. VPC에서 DataSync VPC 서비스 엔드포인트를 사용하는 데 필요한 트래픽을 허용하는 보안 그룹을 구성합니다. 보안 그룹 ARN을 기록해 둡니다(에이전트를 활성화할 때 필요).

   보안 그룹은 에이전트가 VPC 서비스 엔드포인트 및 네트워크 인터페이스(작업을 생성할 때 생성됨)의 프라이빗 IP 주소와 연결하도록 허용해야 합니다.

다음 단계: AWS DataSync 에이전트 활성화

AWS DataSync 에이전트 활성화

AWS DataSync 에이전트 생성을 완료하려면 에이전트를 활성화해야 합니다. 이 단계에서는 에이전트를와 연결합니다 AWS 계정.

> **Note**
>
> 한 AWS 계정 AWS 리전 번에 둘 이상에서 에이전트를 활성화할 수 없습니다.

사전 조건

DataSync 에이전트를 활성화하려면 다음 정보가 있어야 합니다.

- 에이전트를 활성화하는 DataSync 서비스 엔드포인트입니다.

  VPC 서비스 엔드포인트를 사용하는 경우 다음 세부 정보가 필요합니다.

  - VPC 서비스 엔드포인트 ID입니다.
  - VPC 서비스 엔드포인트가 위치한 서브넷입니다.
  - DataSync VPC 서비스 엔드포인트를 사용하는 데 필요한 트래픽을 허용하는 보안 그룹입니다.
- 에이전트의 IP 주소 또는 도메인 이름입니다.

  이를 찾는 방법은 배포하는 에이전트 유형에 따라 다릅니다. 예를 들어 에이전트가 Amazon EC2 인스턴스인 경우, Amazon EC2 콘솔의 인스턴스 페이지로 이동하여 해당 IP 주소를 찾을 수 있습니다.

> **Note**
>
> FIPS VPC 엔드포인트의 경우 AWS CLI 또는 DataSync API를 사용합니다.

활성화 키 가져오기

배포된 DataSync 에이전트에 대한 활성화 키를 얻는 몇 가지 방법이 있습니다. 일부 옵션은 포트 80(HTTP)에서 에이전트에 대한 액세스가 필요합니다. 이러한 옵션 중 하나를 사용하는 경우 에이전트를 활성화하면 DataSync가 포트를 닫습니다.

> **Note**
>
> 에이전트 활성화 키는 사용하지 않으면 30분 후에 만료됩니다.

DataSync console

DataSync 콘솔에서 에이전트를 활성화할 때 DataSync는 에이전트에서 활성화 키 자동 가져오기 옵션을 사용하여 활성화 키를 가져올 수 있습니다.

이 옵션을 사용하려면 브라우저가 포트 80에서 에이전트에 연결할 수 있어야 합니다.

Agent local console

활성화 키를 가져오는 다른 옵션과 달리 이 옵션은 포트 80에서 에이전트에 액세스할 필요가 없습니다.

1. 에이전트 가상 머신(VM) 또는 Amazon EC2 인스턴스의 로컬 콘솔에 로그인합니다.
2. AWS DataSync 활성화 - 구성 기본 메뉴에서 **0**를 입력하여 활성화 키를 가져옵니다.
3. 에이전트를 활성화 AWS 리전 하려는를 입력합니다.
4. 에이전트가 사용하는 서비스 엔드포인트 유형을 입력합니다.
5. 표시되는 활성화 키를 복사합니다.

   예: `F0EFT-7FPPR-GG7MC-3I9R3-27D0H`

   에이전트를 활성화할 때 이 키를 지정합니다.

CLI

표준 Unix 도구를 사용하면 에이전트의 IP 주소에 대한 `curl` 요청을 실행하여 활성화 키를 가져올 수 있습니다.

이 옵션을 사용하려면 클라이언트가 포트 80에서 에이전트에 연결할 수 있어야 합니다. 다음 명령을 실행하여 확인할 수 있습니다.

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

에이전트에 연결할 수 있음을 확인한 후 사용 중인 서비스 엔드포인트 유형에 따라 다음 명령 중 하나를 실행합니다.

- 퍼블릭 서비스 엔드포인트:

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

- FIPS 서비스 엔드포인트:

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

- VPC 서비스 엔드포인트:

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

- FIPS VPC 서비스 엔드포인트:

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

> **Note**
>
> *vpc-endpoint-ip-address*를 찾으려면 Amazon VPC 콘솔을 열고 엔드포인트를 선택한 다음 DataSync VPC 서비스 엔드포인트를 선택합니다. 서브넷 탭에서 VPC 서비스 엔드포인트의 서브넷의 IP 주소를 찾습니다. 이는 엔드포인트의 IP 주소입니다.

이 명령은 활성화 키를 반환합니다. 예제:

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

에이전트를 활성화할 때 이 키를 지정합니다.

에이전트 활성화

DataSync 에이전트를 활성화하는 몇 가지 옵션이 있습니다. 활성화되면 AWS 에서 에이전트를 관리합니다.

DataSync console

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택한 다음, 에에이전트 생성을 선택합니다.
3. 서비스 엔드포인트 섹션에서 다음을 수행하여 에이전트의 서비스 엔드포인트를 지정합니다.
   - 퍼블릭 서비스 엔드포인트의 경우 ***## AWS ##***에서 퍼블릭 서비스 엔드포인트를 선택합니다.
   - FIPS 서비스 엔드포인트의 경우 ***## AWS ##***에서 FIPS 서비스 엔드포인트를 선택합니다.
   - VPC 서비스 엔드포인트의 경우 다음을 수행합니다.
     - AWS PrivateLink를 사용하여 VPC 엔드포인트를 선택합니다.
     - VPC 엔드포인트에서 에이전트가 사용할 VPC 서비스 엔드포인트를 선택합니다.
     - 서브넷에서 VPC 서비스 엔드포인트가 있는 서브넷을 선택합니다.
     - 보안 그룹에서 DataSync VPC 서비스 엔드포인트를 사용하는 데 필요한 트래픽을 허용하는 보안 그룹을 선택합니다.
4. 활성화 키 섹션에서 다음 중 하나를 수행하여 에이전트의 활성화 키를 지정합니다.
   - 에이전트에서 DataSync용 활성화 키 자동 가져오기를 선택하여 키를 가져옵니다.

- 에이전트 주소에서 에이전트의 IP 주소 또는 도메인 이름을 입력합니다.
- Get key를 선택합니다.

  활성화에 실패하면 사용 중인 서비스 엔드포인트 유형에 따라 네트워크 구성을 확인합니다.

- 브라우저와 에이전트를 연결하지 않으려면 에이전트 활성화 키 수동 입력을 선택합니다.
  - 에이전트 로컬 콘솔에서 또는 `curl` 명령을 사용하여 키를 가져옵니다.
  - DataSync 콘솔로 돌아가서 활성화 키 필드에 키를 입력합니다.

5. (권장) 에이전트 이름에서 에이전트에 기억할 수 있는 이름을 지정합니다.
6. (선택 사항) 태그에는 에이전트을 태그할 키 및 값 필드에 값을 입력합니다.

   태그는 AWS 리소스 관리, 필터링 및 검색에 도움이 됩니다.
7. Create agent(에이전트 생성)을 선택합니다.
8. 에이전트 페이지에서 사용 중인 서비스 엔드포인트 유형이 올바른지 확인합니다.

> **Note**
>
> 이 시점에서는 에이전트가 오프라인 상태임을 알 수 있습니다. 이 문제는 에이전트를 활성화한 후 잠시 후에 발생합니다.

AWS CLI

1. 활성화 키를 가져오면 사용 중인 서비스 엔드포인트 유형에 따라 다음 `create-agent` 명령 중 하나를 복사합니다.

   - 퍼블릭 또는 FIPS 서비스 엔드포인트:

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

   - VPC 또는 FIPS VPC 서비스 엔드포인트:

   ```
   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. `--activation-key`에서 에이전트 활성화 키를 지정합니다.
3. (권장) `--agent-name`에서 기억할 수 있는 에이전트의 이름을 지정합니다.
4. VPC 서비스 엔드포인트를 사용하는 경우 다음 옵션을 지정합니다.
   - `--vpc-endpoint-id`에서 사용 중인 VPC 서비스 엔드포인트의 ID를지정합니다.
   - `--subnet-arns`에서 VPC 서비스 엔드포인트가 위치한 서브넷의 ARN을 지정합니다.
   - `--security-group-arns`에서 DataSync VPC 서비스 엔드포인트를 사용하는 데 필요한 트래픽을 허용하는 보안 그룹의 ARN을 지정합니다.
5. `create-agent` 명령을 실행합니다.

   방금 활성화한 에이전트의 ARN에 대한 응답을 받습니다. 예제:

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

6. `list-agents` 명령을 실행하여 에이전트가 활성화되었는지 확인합니다.

```
aws datasync list-agents
```

> **Note**
>
> 이 시점에서는 에이전트 `Status`가 `OFFLINE` 상태임을 알 수 있습니다. 이 문제는 에이전트를 활성화한 후 잠시 후에 발생합니다.

DataSync API

활성화 키를 가져오면 CreateAgent 작업을 사용하여 에이전트를 활성화합니다.

> **Note**
>
> 완료되면 에이전트가 오프라인 상태일 수 있습니다. 이 문제는 에이전트를 활성화한 후 잠시 후에 발생합니다.

다음 단계

- 스토리지 시스템 및 DataSync 서비스에 대한 에이전트의 연결을 확인합니다.
- 에이전트를 활성화하는 데 문제가 발생하면 문제 해결 도움을 받으세요.
- 에이전트와 함께 사용할 DataSync 위치를 생성합니다. 온프레미스 또는 기타 클라우드 위치일 수 있습니다.

에이전트의 네트워크 연결 확인

AWS DataSync 에이전트를 활성화한 후에는 에이전트가 스토리지 시스템 및 DataSync 서비스에 네트워크로 연결되어 있는지 확인합니다.

에이전트의 로컬 콘솔 액세스

에이전트의 로컬 콘솔에 액세스하는 방법은 사용 중인 에이전트 유형에 따라 다릅니다.

로컬 콘솔(VMware ESXi, Linux KVM 또는 Microsoft Hyper-V) 액세스

보안상의 이유로 DataSync 에이전트 VM(가상 머신)의 로컬 콘솔에 원격으로 연결할 수 없습니다.

- 로컬 콘솔에 처음 로그인하는 경우, 기본 보안 인증 정보를 사용하여 로그인합니다. 기본 사용자 이름과 암호는 각각 **admin** 및 **password**입니다.

  > **Note**
  >
  > 기본 암호를 변경하는 것이 좋습니다. 이렇게 하려면 콘솔 기본 메뉴에서(**5**또는 VMware VM의 경우 **6**)를 입력한 다음 `passwd`명령을 실행하여 암호를 변경합니다.

로컬 콘솔 액세스(Amazon EC2)

Amazon EC2 에이전트의 로컬 콘솔에 연결하려면 SSH를 사용해야 합니다.

시작하기 전에: EC2 인스턴스의 보안 그룹이 SSH(TCP 포트 22)를 통한 액세스를 허용하는지 확인합니다.

1. 터미널을 열고 다음 `ssh`명령을 복사합니다.

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

- */path/key-pair-name*의 경우 인스턴스에 연결하는 데 필요한 프라이빗 키의 경로와 파일 이름(`.pem`)을 지정합니다.
- *instance-user-name*의 경우 `admin`를 지정합니다.
- *instance-public-ip-address*의 경우, 인스턴스의 퍼블릭 IP 주소를 지정합니다.

2. `ssh` 명령을 실행하여 인스턴스에 연결합니다.

연결되면 에이전트의 로컬 콘솔 기본 메뉴가 표시됩니다.

에이전트의 스토리지 시스템 연결 확인

DataSync 에이전트가 스토리지 시스템에 연결할 수 있는지 테스트합니다. 자세한 내용은 1. 스토리지 시스템과 에이전트 간의 네트워크 연결 단원을 참조하십시오.

1. 에이전트의 로컬 콘솔에 액세스합니다.
2. AWS DataSync 활성화 - 구성 기본 메뉴에서 **3**을 입력합니다.
3. 다음 옵션 중 하나를 입력합니다.
   a. NFS 서버 연결을 테스트하려면 **1**을 입력합니다.
   b. SMB 서버 연결을 테스트하려면 **2**을 입력합니다.
   c. 객체 스토리지 서버 연결을 테스트하려면 **3**을 입력합니다.
   d. HDFS 연결을 테스트하려면 **4**을 입력합니다.
   e. Microsoft Azure Blob Storage 연결을 테스트하려면 **5**을 입력합니다.
4. 스토리지 서버의 IP 주소 또는 도메인 이름을 입력합니다.

   IP 주소 또는 도메인 이름을 입력할 때는 다음 사항에 유의하세요.

   - 프로토콜은 포함하지 않습니다. 예를 들어 **`https://mystorage.com`**대신 **`mystorage.com`**을 입력하십시오.
   - HDFS의 경우 Hadoop 클러스터에 있는 NameNode 또는 DataNode의 IP 주소 또는 도메인 이름을 입력합니다.
5. 요청된 경우 스토리지 서버에 연결하기 위한 TCP 포트(예: **443**)를 입력합니다.

연결 테스트의 PASSED 또는 FAILED 여부를 확인합니다.

에이전트의 DataSync 서비스 연결 확인

DataSync 에이전트가 DataSync 서비스에 연결할 수 있는지 테스트합니다. 자세한 내용은 2. 에이전트와 DataSync 서비스 간의 네트워크 연결 단원을 참조하십시오.

1. 에이전트의 로컬 콘솔에 액세스합니다.
2. 네트워크 연결 테스트를 시작하려면 AWS DataSync 활성화 - 구성 기본 메뉴에서 **2**를 입력합니다.

   에이전트가 활성화되면 활성화된 에이전트 정보에서 리전 및 엔드포인트 유형을 가져오므로 추가 사용자 입력 없이 네트워크 연결 테스트 옵션을 시작할 수 있습니다.
3. 에이전트가 사용하는 DataSync 서비스 엔드포인트의 유형을 입력합니다.

   a. 퍼블릭 서비스 엔드포인트에 에이전트가 활성화된 **1** 및 AWS 리전 를 입력합니다.

   b. FIPS 서비스 엔드포인트의 경우 **2**과 에이전트가 활성화된 리전을 입력합니다.

   c. VPC 서비스 엔드포인트에 **3**을 입력합니다.

   d. FIPS VPC 서비스 엔드포인트에 **4**를 입력합니다.

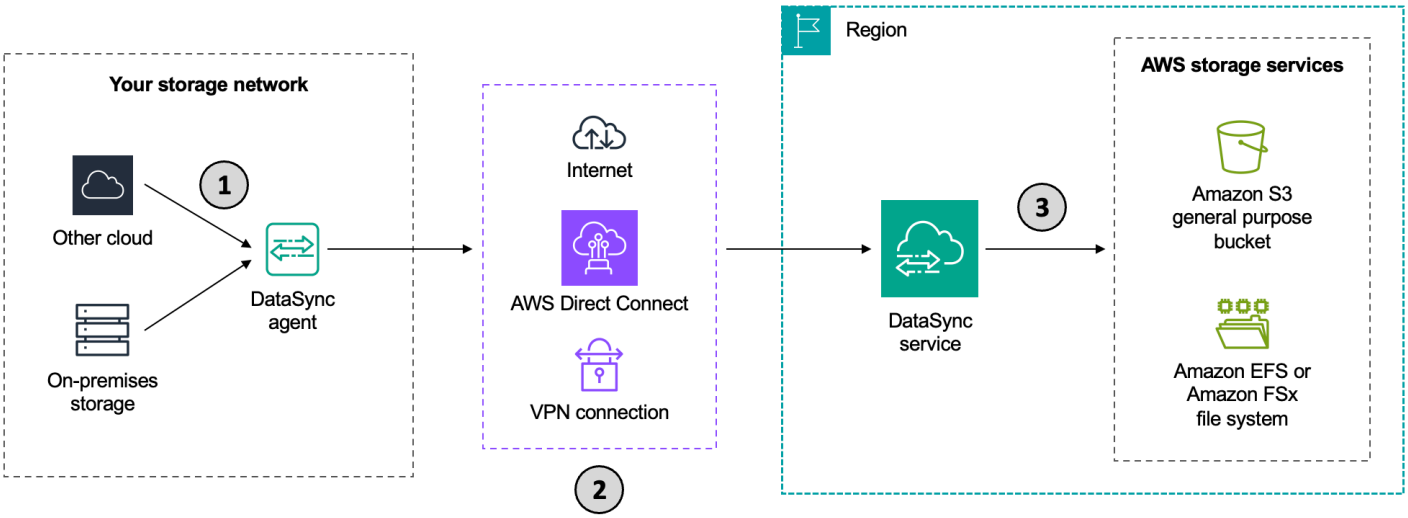
   PASSED 또는 FAILED 메시지가 표시됩니다.
4. FAILED 메시지가 표시되면 네트워크 구성을 확인합니다. 자세한 내용은 AWS DataSync 네트워크 요구 사항 단원을 참조하십시오.

다음 단계

에이전트와 함께 사용할 DataSync 위치를 생성합니다. 온프레미스 또는 기타 클라우드 위치일 수 있습니다.

AWS DataSync 전송을 위해 네트워크 연결

AWS DataSync 에이전트가 필요한 경우 데이터 전송을 위해 여러 네트워크 연결을 설정해야 합니다. 다음 다이어그램은 스토리지 시스템(온프레미스, 다른 클라우드 또는 엣지)에서 AWS 스토리지 서비스로 DataSync 전송의 세 가지 네트워크 연결을 보여줍니다.



1. 스토리지 시스템과 에이전트 간의 네트워크 연결

DataSync 에이전트는 온프레미스 스토리지 또는 다른 클라우드의 스토리지에 연결됩니다. 자세한 내용은 온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항 단원을 참조하십시오.

2. 에이전트와 DataSync 서비스 간의 네트워크 연결

에이전트를 DataSync 서비스에 연결하는 데는 몇 가지 측면이 있습니다. 먼저 스토리지 위치와 간에 네트워크 연결을 설정해야 합니다 AWS. 그런 다음 에이전트는 DataSync와 통신하려면 서비스 엔드포인트가 필요합니다.

목차

- 에 스토리지 네트워크 연결 AWS
- 서비스 엔드포인트 선택

에 스토리지 네트워크 연결 AWS

DataSync를 사용할 때는 스토리지 네트워크를 AWS에 연결하기 위해 다음 옵션을 고려하세요.

- Direct Connect - Direct Connect를 사용하면 스토리지 네트워크와 AWS간에 전용 연결을 생성할 수 있습니다. DataSync 관점에서 다음을 수행할 수 있습니다.
  - 프라이빗 경로를 통해 데이터를 가상 프라이빗 클라우드(VPC)로 전송하면 퍼블릭 인터넷을 통한 라우팅이 방지됩니다.
  - 가상 프라이빗 네트워크(VPN)를 사용하여 스토리지 네트워크를에 연결하는 것보다 더 예측 가능한 연결을 확보합니다 AWS (특히 에이전트가 Amazon EC2 인스턴스인 경우).
  - 퍼블릭, Federal Information Processing Standard(FIPS) 또는 VPC 엔드포인트를 포함한 모든 유형의 DataSync 서비스 엔드포인트를 사용합니다.

  자세한 내용은 를 사용한 DataSync 아키텍처 및 라우팅 예제 Direct Connect 단원을 참조하십시오.
- VPN - VPN(예:)을 사용하여 스토리지 네트워크를 AWS 에 연결할 수 있습니다AWS Site-to-Site VPN.
- 퍼블릭 인터넷 - 퍼블릭 또는 FIPS 서비스 엔드포인트를 사용하여 인터넷을 통해 스토리지 네트워크를 DataSync에 직접 연결할 수 있습니다.

서비스 엔드포인트 선택

에이전트는 서비스 엔드포인트를 사용하여 DataSync와 통신합니다. 자세한 내용은 AWS DataSync 에이전트의 서비스 엔드포인트 선택 단원을 참조하십시오.

3. DataSync 서비스와 AWS 스토리지 서비스 간의 네트워크 연결

DataSync를 AWS 스토리지 서비스에 연결하려면 DataSync 서비스가 S3 버킷 또는 파일 시스템에 액세스할 수 있는지 확인하기만 하면 됩니다. 자세한 내용은 AWS 스토리지 서비스에 대한 네트워크 요구 사항 단원을 참조하십시오.

DataSync 에이전트가 필요하지 않은 경우의 네트워킹

DataSync 에이전트가 필요하지 않은 전송의 경우, DataSync 서비스가 전송을 수행하는 양쪽 AWS 스토리지 서비스에 액세스할 수 있는지만 확인하면 됩니다. 자세한 내용은 AWS 스토리지 서비스에 대한 네트워크 요구 사항 단원을 참조하십시오.

DataSync 트래픽이 네트워크를 통과하는 방식 및 위치

DataSync에는 데이터 플레인 및 컨트롤 플레인 트래픽이 있습니다. DataSync 트래픽을 분리하려는 경우 이러한 각 흐름이 네트워크를 통해 어떻게 흐르는지 알아야 합니다.

- 데이터 플레인 트래픽 - 스토리지 위치 간에 이동하는 파일 또는 객체 데이터를 포함합니다. 대부분의 경우 사용자가 작업을 생성할 때 DataSync가 자동으로 생성하고 관리하는 네트워크 인터페이스를 통해 데이터 플레인 트래픽이 라우팅됩니다. 이러한 네트워크 인터페이스가 생성되는 위치는 송수신되는 AWS 스토리지 서비스의 유형과 DataSync 에이전트가 사용하는 서비스 엔드포인트에 따라 달라집니다.
- 컨트롤 플레인 트래픽 - DataSync 리소스에 대한 관리 활동을 포함합니다. 이 트래픽은 에이전트가 사용하는 서비스 엔드포인트를 통해 라우팅됩니다.

DataSync의 네트워크 보안

전송 중에 스토리지 데이터(메타데이터 포함)를 보호하는 방법에 대한 자세한 내용은 AWS DataSync 전송 중 암호화 섹션을 참조하세요.

AWS DataSync 네트워크 요구 사항

네트워크 구성은 AWS DataSync설정의 중요한 단계입니다. 네트워크 구성은 작업 중인 스토리지 시스템 유형과 같은 여러 요소에 따라 달라집니다. 또한 사용할 DataSync 서비스 엔드포인트의 종류에 따라 달랍니다.

IPv6 지원

DataSync는 IPv4 및 IPv6 네트워크와 호환성을 위해 듀얼 스택을 지원합니다. IPv6 지원은 서비스가 제공되는 모든 AWS 리전 에서 사용할 수 있습니다. DataSync는 다음 데이터 소스와 함께 IPv6 주소 사용을 지원합니다.

- Elastic File System(EFS)
- NFS(Network File System)
- Server Message Block(SMB)
- 객체 스토리지

온프레미스 스토리지를 위한 IPv6 호환 에이전트

IPv6 네트워크 환경에서 DataSync를 사용하려면 IPv6 호환 에이전트를 사용해야 합니다. 이러한 에이전트는 IPv4 및 IPv6 연결을 모두 지원하며 다양한 네트워크 환경에 맞게 조정됩니다.

- IPv6 전용 네트워크의 경우 - 구성을 변경할 필요가 없습니다.
- IPv4 전용 네트워크의 경우 - 구성을 변경할 필요가 없습니다.
- 듀얼 스택(IPv4 및 IPv6 모두) 네트워크의 경우 - 에이전트가 프로토콜을 선택하거나 기본 설정에 따라 수동으로 구성할 수 있습니다.

듀얼 스택 네트워크 고려 사항

다음과 같은 방법으로 로컬 콘솔을 통해 에이전트의 동작을 사용자 지정할 수 있습니다.

- 에이전트가 IPv6를 사용하여 로컬 파일 시스템 또는 DataSync 서비스에 연결할 수 없도록 IPv6를 비활성화합니다.
- 데이터 전송에 사용할 에이전트의 IP 버전을 설정합니다.
  - IPv6로 설정하여 에이전트가 데이터 전송에 IPv6만 사용하도록 합니다.
  - IPv4로 설정하여 에이전트가 데이터 전송에 IPv4만 사용하도록 합니다.
  - 자동(기본값 복원)으로 설정하여 에이전트가 데이터 전송을 위한 프로토콜 버전(IPv4 또는 IPv6)을 자동으로 선택하도록 합니다.

에이전트 IP 버전 설정에 대한 자세한 내용은 the section called “에이전트에 대한 유지 관리 수행”을(를) 참조하세요.

> **Important**
>
> 2025년 7월 16일 이전에 다운로드한 이미지로 빌드된 에이전트는 IPv6를 지원하지 않습니다.

온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항

다음 네트워크 요구 사항은 온프레미스, 자체 관리형 및 기타 클라우드 스토리지 시스템에 적용될 수 있습니다. 일반적으로 사용자가 관리하거나 다른 클라우드 공급자가 관리할 수 있는 스토리지 시스템입니다.

> **Note**
>
> 네트워크에 따라 DataSync 에이전트가 스토리지에 연결하려면 여기에 나열된 포트 이외의 포트에서 트래픽을 허용해야 할 수 있습니다.

From	목적	프로토콜	포트	DataSync에서 사용하는 방법
DataSync 에이전트	NFS 파일 서버	TCP	2049(NFS 버전 4.1 및 4.0용) 111 및 2049(NFS 버전 3.x용)	NFS 파일 서버를 마운트합니다. DataSync는 NFS 버전 3.x, 4.0, 및 4.1을 지원합니다.
DataSync 에이전트	SMB 파일 서버	TCP	139 또는 445	SMB 파일 서버를 마운트합니다. DataSync는 SMB 버전 1.0 이상을 지원합니다. 보안상의 이유로 SMB 버전 3.0.2 이상을 사용하는 것이 좋습니다. SMB 1.0과 같은 이전 버전에는 알려진 보안 취약성이 포함되어 있어, 공격자가 데이터를 손상시키기 위해 이를 악용할 수 있습니다.
DataSync 에이전트	객체 스토리지	TCP	443(HTTPS) 또는 80(HTTP)	온프레미스 또는 다른 클라우드에서 Amazon S3 호환 객체 스토리지에 액세스합니다.

From	목적	프로토콜	포트	DataSync에서 사용하는 방법
			Note 객체 스토리지에 따라 비표준 HTTPS 및 HTTP 포트(예: 8443 또는 8080)에서 트래픽을 허용해야	

From	목적	프로토콜	포트	DataSync에서 사용하는 방법
			할 수 있습니다.	
DataSync 에이전트	Hadoop 클러스터	TCP	NameNode 포트(기본값은 8020) 대부분의 클러스터에서는 Hadoop 배포에 따라 `core-site.xml` 파일의 `fs.default` 또는 `fs.default.name` 속성에서 이 포트 번호를 찾을 수 있습니다.	Hadoop 클러스터의 NameNode에 액세스합니다. HDFS 위치를 생성할 때 사용되는 포트를 지정합니다.

From	목적	프로토콜	포트	DataSync에서 사용하는 방법
DataSync 에이전트	Hadoop 클러스터	TCP	DataNode 포트(기본값은 50010) 대부분의 클러스터에서는 `hdfs-site.xml` 파일의 `dfs.datanode.address` 속성에서 이 포트 번호를 찾을 수 있습니다.	Hadoop 클러스터의 DataNodes에 액세스합니다. DataSync 에이전트는 사용할 포트를 자동으로 결정합니다.
DataSync 에이전트	Hadoop 키 관리 서버(KMS)	TCP	KMS 포트(기본값은 9600)	Hadoop 클러스터의 KMS에 액세스합니다.
DataSync 에이전트	Kerberos 키 분포 센터(KDC) 서버	TCP	KDC 포트(기본값은 88)	Kerberos 영역으로 인증합니다. 이 포트는 Kerberos 인증을 사용하는 HDFS 및 SMB 위치에서만 사용됩니다.
DataSync 에이전트	스토리지 시스템의 관리 인터페이스	TCP	네트워크에 따라 다름	스토리지 시스템에 연결합니다.

AWS 스토리지 서비스에 대한 네트워크 요구 사항

전송 중에 DataSync가 AWS 스토리지 서비스에 연결하는 데 필요한 네트워크 포트는 다양합니다.

From	목적	프로토콜	포트
DataSync 서비스	Amazon EFS	TCP	2049
DataSync 서비스	FSx for Windows File Server	Windows File Server 파일 시스템 액세스 제어를 참조하세요.	
DataSync 서비스	Lustre용 FSx	FSx for Lustre 파일 시스템 액세스 제어를 참조하세요.	
DataSync 서비스	FSx for OpenZFS	FSx for OpenZFS 파일 시스템 액세스 제어를 참조하세요.	
DataSync 서비스	FSx for ONTAP	TCP	111, 635 및 2,049(NFS) 445(SMB)
DataSync 서비스	Amazon S3	해당 없음(DataSync는 사용자를 대신하여 S3 버킷에 연결)	

퍼블릭 또는 FIPS 서비스 엔드포인트의 네트워크 요구 사항

DataSync 에이전트는 공용 또는 FIPS 서비스 엔드포인트를 사용할 때 다음 네트워크 액세스가 필요합니다. 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링하거나 제한하는 경우, 방화벽 또는 라우터가 이 엔드포인트를 허용하도록 구성합니다.

From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
웹 브라우저	DataSync 에이전트	TCP	80(HTTP)	브라우저가 DataSync 에이전트 활성화 키를 가져오	해당 사항 없음

From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
				는 데 사용됩니다. 활성화되면 DataSync는 에이전트의 포트 80을 닫습니다. 에이전트에 대한 퍼블릭 액세스에는 포트 80이 필요하지 않습니다. 포트 80에 액세스하는 데 필요한 권한 수준은 네트워크 구성에 따라 다릅니다. **Note** 브라우저와 에이전트 간의 연결 없이 활성화 키를 가져올 수 있습니다. 자세한 내용은 활성화 키 가져오기 단원을	

From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
				참조하십시오.	
DataSync 에이전트	Amazon CloudFront	TCP	443(HTTP)	활성화 전에 DataSync 에이전트를 부트스트랩하는 데 도움이 됩니다. 기본 모드 에이전트에만 필요합니다.	AWS 리전: • `d3dvvaliwoko8h.cloudfront.net` AWS GovCloud (US) 리전: • `s3.us-gov-west-1.amazonaws.com/fmrsendpoints-endpoints bucket-go4p5gpna6sk`
DataSync 에이전트	AWS	TCP	443(HTTP)	DataSync 에이전트를 활성화하고 AWS 계정와 연결합니다. 정품 인증 후 퍼블릭 엔드포인트를 차단할 수 있습니다.	*activation-region* 는 DataSync 에이전트를 활성화 AWS 리전 하는 입니다. 퍼블릭 엔드포인트 정품 인증: • `activation.datasync.` *activation-region* `.amazonaws.com` FIPS 엔드포인트 정품 인증: • `activation.datasync-fips.` *activation-region* `.amazonaws.com`

From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
DataSync 에이전트	AWS	TCP	443(HTTP)	DataSync 에이전트와 DataSync 서비스 엔드포인트 간의 통신을 허용합니다. 자세한 내용은 AWS DataSync 에이전트의 서비스 엔드포인트 선택 단원을 참조하세요.	*activation-region* 는 DataSync 에이전트를 활성화 AWS 리전 하는 입니다. DataSync를 사용하는 용도에 따라 여기에 나열된 모든 엔드포인트에 대한 액세스를 허용할 필요가 없을 수도 있습니다. DataSync 컨트롤 플레인 엔드포인트: • 퍼블릭 엔드포인트: `cp.datasync.` *activation-region*`.amazonaws.com` • FIPS 엔드포인트: `cp.datasync-fips.` *activation-region*`.amazonaws.com` DataSync 데이터 영역 엔드포인트(전송 작업에만 해당): • 기본 모드 에이전트: *your-task-id* `.datasync-dp.` *activation-region*`.amazonaws.com` 향상된 모드 에이전트: **.*.your-task-id.** `.datasync-dp.` *activation-region* `.amazonaws.com`

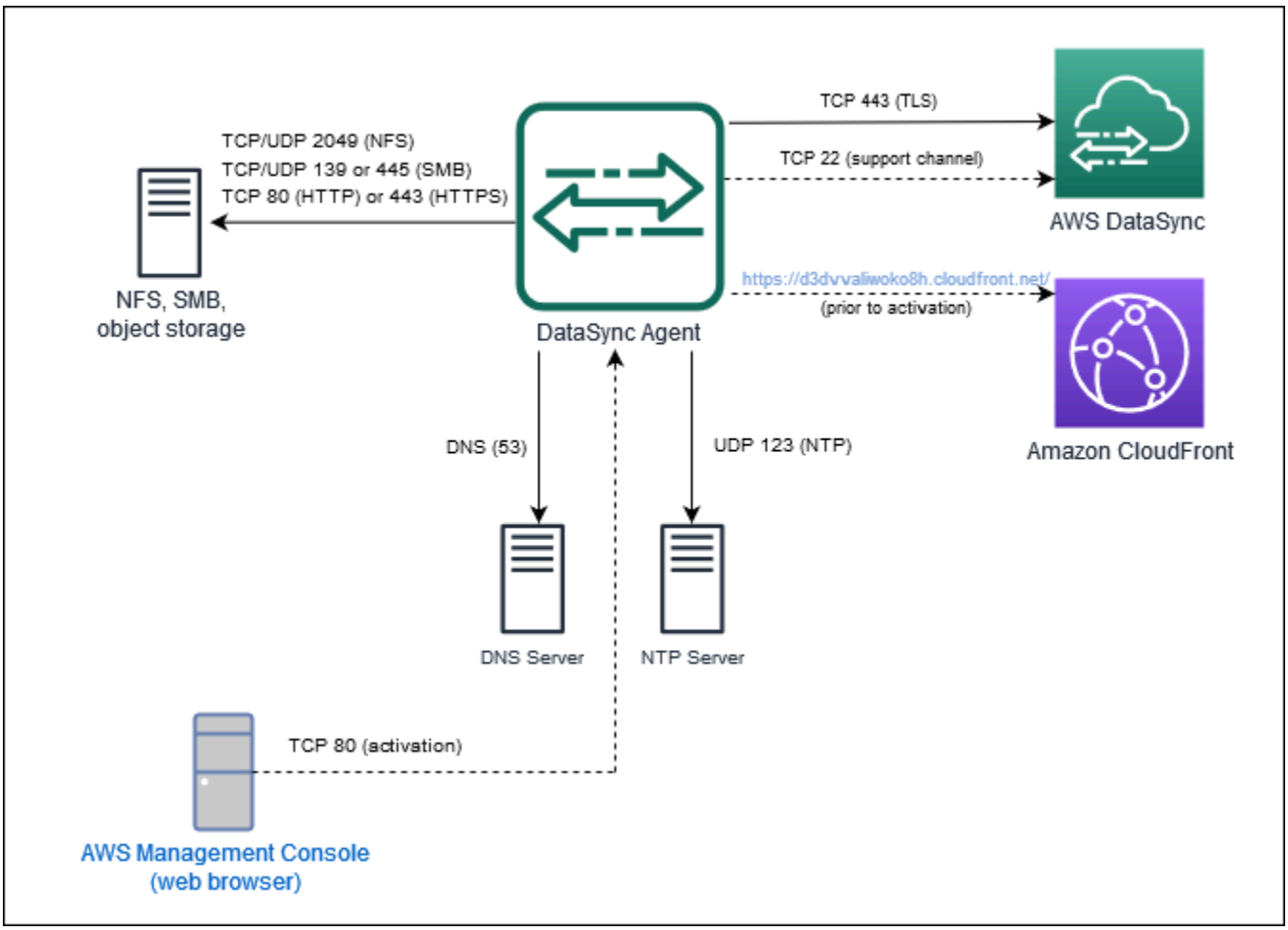
From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
클라이언트	AWS	TCP	443(HTTP)	DataSync API 요청을 수행할 수 있습니다.	*activation-region* 는 DataSync 에이전트를 활성화 AWS 리전 하는 입니다. 퍼블릭 엔드포인트: • datasync. *activation-region*.amazonaws.com FIPS 엔드포인트: • datasync-fips. *activation-region* .amazonaws.com

From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
DataSync 에이전트	AWS	TCP	443(HTTP)	DataSync 에이전트가 업데이트를 가져올 수 있도록 허용합니다 AWS. 자세한 내용은 AWS DataSync 에이전트 관리 단원을 참조하십시오.	*activation-region* 는 DataSync 에이전트를 활성화 AWS 리전 하는 입니다. 기본 모드 에이전트: • 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 향상된 모드 에이전트: • *.s3.dualstack. *activation-region*.amazonaws.com

From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
DataSync 에이전트	DNS(Domain Name Service) 서버	TCP/UDP	53(DNS)	DataSync 에이전트와 DNS 서버 간의 통신에 사용됩니다.	해당 사항 없음
DataSync 에이전트	AWS	TCP	22(지원 채널)	AWS Support가 DataSync 에이전트에 액세스하여 문제를 해결할 수 있도록 허용합니다. 정상적으로 작동하면 이 포트를 열지 않아도 됩니다.	기본 모드 에이전트: • 상용 리전: `54.201.223.107` • GovCloud 리전: `52.222.99.142` 향상된 모드 에이전트: • 상용 리전: `support.datasync.us-east-1.amazonaws.com` • GovCloud 리전: `support.datasync.us-gov-west-1.amazonaws.com`

From	목적	프로토콜	포트	사용 방법	액세스한 엔드포인트
DataSync 에이전트	NTP(Network Time Protocol) 서버	UDP	123(NTP)	로컬 시스템이 VM 시간을 호스트 시간과 동기화하는 데 사용됩니다.	NTP: • `0.amazon.pool.ntp.org` • `1.amazon.pool.ntp.org` • `2.amazon.pool.ntp.org` • `3.amazon.pool.ntp.org` **Note** 로컬 콘솔을 통해 다른 NTP 서버를 사용하도록 VM 에이전트의 기본 NTP 구성을 변경하려면 에이전트 시스템 시간 서버 구성 보기 및 관리을 참조하십시오.

다음 다이어그램은 퍼블릭 또는 FIPS 서비스 엔드포인트를 사용할 때 DataSync에 필요한 포트를 보여줍니다.



VPC 또는 FIPS VPC 서비스 엔드포인트에 대한 네트워크 요구 사항

Virtual Private Cloud(VPC) 엔드포인트는 에이전트와 간에 인터넷을 통과하거나 퍼블릭 IP 주소를 사용하지 AWS 않는 프라이빗 연결을 제공합니다. 이렇게 하면 패킷이 네트워크에 들어오거나 나가는 것도 방지할 수 있습니다. 자세한 내용은 VPC 서비스 엔드포인트 선택 단원을 참조하십시오.

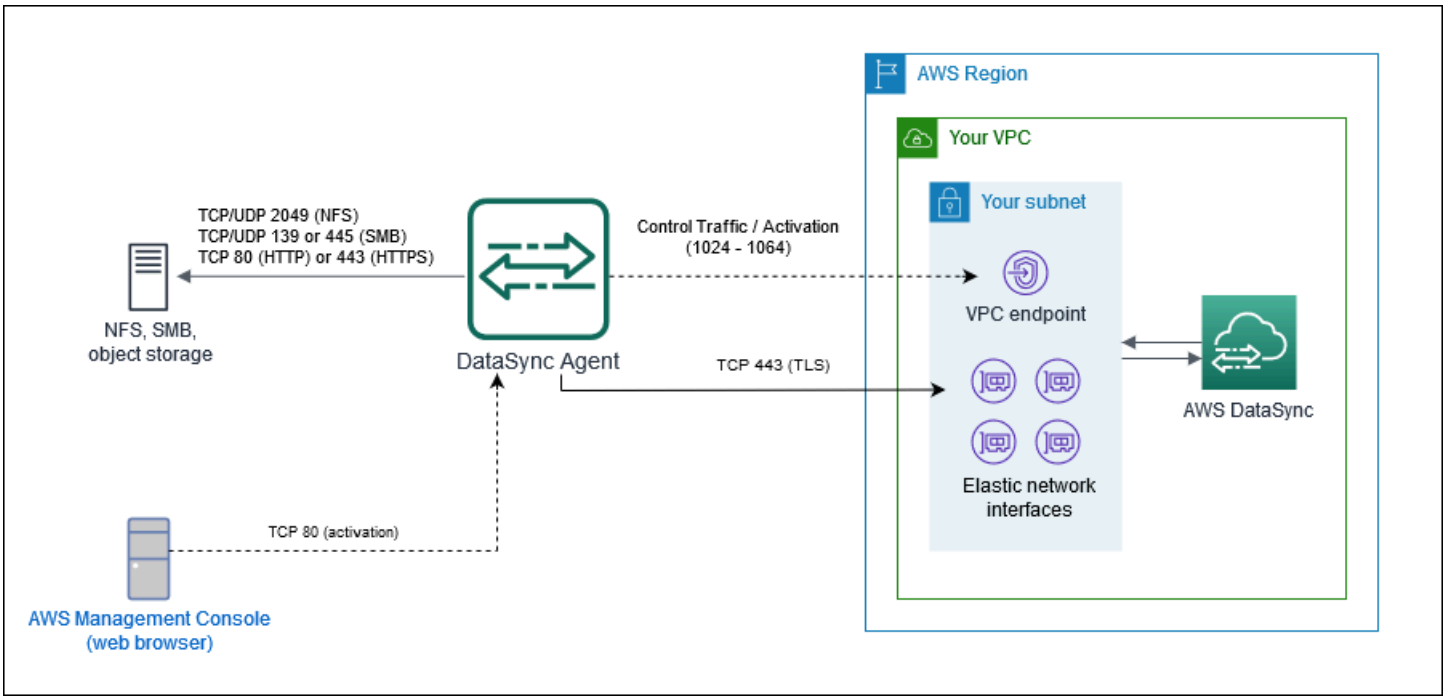
에이전트가 VPC 서비스 엔드포인트를 사용하려면 DataSync에서 다음 포트가 필요합니다.

From	목적	프로토콜	포트	사용 방법
웹 브라우저	내 DataSync 에이전트	TCP	80(HTTP)	브라우저가 에이전트 활성화 키를 가져오는 데 사용됩니다. 활성화되면 DataSync는 에이전트의 포트 80을 닫습니다.

From	목적	프로토콜	포트	사용 방법
				에이전트에 대한 퍼블릭 액세스에는 포트 80이 필요하지 않습니다. 포트 80에 액세스하는데 필요한 권한 수준은 네트워크 구성에 따라 다릅니다. **Note** 브라우저와 에이전트 간의 연결 없이 활성화 키를 가져올 수 있습니다. 자세한 내용은 활성화 키 가져오기 단원을 참조하십시오.
DataSync 에이전트	DataSync VPC 서비스 엔드포인트 엔드포인트의 IP 주소를 찾으려면 Amazon VPC 콘솔을 열고 엔드포인트를 선택한 다음 DataSync VPC 서비스 엔드포인트를 선택합니다. 서브넷 탭에서 VPC 서비스 엔드포인트의 서브넷의 IP 주소를 찾습니다. 이는 엔드포인트의 IP 주소입니다.	TCP	1024~1064	컨트롤 플레인 트래픽용

From	목적	프로토콜	포트	사용 방법
DataSync 에이전트	DataSync 작업의 네트워크 인터페이스 이러한 인터페이스의 IP 주소를 찾으려면 네트워크 인터페이스 보기 섹션을 참조하세요.	TCP	443(HTTPS)	데이터 플레인 트래픽용
DataSync 에이전트	DataSync VPC 서비스 엔드포인트	TCP	22(지원 채널)	AWS Support 가 문제 해결을 위해 DataSync 에이전트에 액세스할 수 있도록 허용하려면 기본 모드 에이전트에만 필요합니다. 정상적으로 작동하면 이 포트를 열지 않아도 됩니다.

다음 다이어그램은 VPC 서비스 엔드포인트를 사용할 때 DataSync에 필요한 포트를 보여줍니다.



AWS DataSync 전송을 위한 네트워크 인터페이스

생성하는 모든 작업에 대해는 데이터 전송 트래픽에 대한 네트워크 인터페이스를 AWS DataSync 자동으로 생성하고 관리합니다. DataSync가 생성하는 네트워크 인터페이스 수와 생성 위치는 다음과 같은 전송 작업 세부 정보에 따라 달라집니다.

- 작업에 따른 DataSync 에이전트 필요 여부
- 소스 및 대상 위치(데이터를 주고받는 위치).
- 에이전트가 사용하는 서비스 엔드포인트의 유형.

각 네트워크 인터페이스는 서브넷의 단일 IP 주소를 사용합니다. 네트워크 인터페이스가 많을수록 필요한 IP 주소도 많아집니다. 다음 표를 사용하여 서브넷에 작업에 필요한 충분한 IP 주소가 있는지 확인하세요.

에이전트와의 전송을 위한 네트워크 인터페이스

일반적으로 AWS 스토리지 서비스와 그렇지 않은 스토리지 시스템 간에 데이터를 복사할 때는 DataSync 에이전트가 필요합니다 AWS.

Location	기본적으로 생성되는 네트워크 인터페이스	퍼블릭 또는 FIPS 엔드포인트를 사용할 때 네트워크 인터페이스가 생성되는 위치	프라이빗 (VPC) 엔드포인트를 사용할 때 네트워크 인터페이스가 생성되는 위치
Amazon S3	4	N/A 1	DataSync 에이전트를 활성화할 때 지정하는 서브넷입니다.
Amazon EFS	4	Amazon EFS 위치를 생성할 때 지정하는 서브넷입니다.	
Amazon FSx for Windows File Server	4	파일 시스템의 기본 파일 서버와 동일한 서브넷입니다.	
Amazon FSx for Lustre	4	파일 시스템과 동일한 서브넷입니다.	

Location	기본적으로 생성되는 네트워크 인터페이스	퍼블릭 또는 FIPS 엔드포인트를 사용할 때 네트워크 인터페이스가 생성되는 위치	프라이빗 (VPC) 엔드포인트를 사용할 때 네트워크 인터페이스가 생성되는 위치
Amazon FSx for OpenZFS	4	파일 시스템과 동일한 서브넷입니다.	
Amazon FSx for NetApp ONTAP	4	파일 시스템과 동일한 서브넷입니다.	

[1] DataSync 서비스가 S3 버킷과 직접 통신하므로 네트워크 인터페이스는 필요하지 않습니다.

에이전트 없이 전송을 위한 네트워크 인터페이스

AWS 서비스간에 데이터를 복사할 때는 DataSync 에이전트가 필요하지 않습니다.

총 네트워크 인터페이스의 수는 전송 시 DataSync 위치에 따라 다릅니다. 예를 들어 Amazon EFS와 FSx for Lustre 파일 시스템 간 전송에는 네 개의 네트워크 인터페이스가 필요합니다. 한편, FSx for Windows File Server와 S3 버킷 간 전송에는 두 개의 네트워크 인터페이스가 필요합니다.

Location	기본적으로 생성되는 네트워크 인터페이스	네트워크 인터페이스가 생성되는 위치
Amazon S3	N/A [1]	N/A [1]
Amazon EFS	2	Amazon EFS 위치를 생성할 때 지정하는 서브넷입니다.
FSx for Windows File Server	2	파일 시스템의 기본 파일 서버와 동일한 서브넷입니다.
Lustre용 FSx	2	파일 시스템과 동일한 서브넷입니다.
FSx for OpenZFS	2	파일 시스템과 동일한 서브넷입니다.

Location	기본적으로 생성되는 네트워크 인터페이스	네트워크 인터페이스가 생성되는 위치
FSx for ONTAP	2	파일 시스템과 동일한 서브넷입니다.

[1] DataSync 서비스가 S3 버킷과 직접 통신하므로 네트워크 인터페이스는 필요하지 않습니다.

네트워크 인터페이스 보기

DataSync 전송 작업에 할당된 네트워크 인터페이스를 보려면 다음 중 하나를 수행하세요.

- DescribeTask 작업을 사용합니다. 작업이 `SourceNetworkInterfaceArns`및 `DestinationNetworkInterfaceArns`로 반환되고 다음과 같은 응답이 나타납니다.

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

  이 예에서 네트워크 인터페이스 ID는 `eni-f012345678abcdef0`입니다.
- Amazon EC2 콘솔에서 작업 ID(예: `task-f012345678abcdef0`)를 검색하여 해당 네트워크 인터페이스를 찾을 수 있습니다.

를 사용한 DataSync 아키텍처 및 라우팅 예제 Direct Connect

Direct Connect를 AWS DataSync 전송과 함께 사용할 경우 다음 네트워크 아키텍처를 고려하세요.

> **Tip**
>
> 네트워크가 전송 게이트웨이를 사용하는 경우 비용을 최적화하기 위해 DataSync 전송의 논리적 경로를 분리하는 것이 좋습니다(특히 대량의 데이터를 마이그레이션하는 경우).
> 예를 들어 온프레미스 네트워크와 가상 프라이빗 클라우드(VPC) 간의 정상 트래픽에 AWS Transit Gateway를 사용하는 경우 DataSync 트래픽이 전송 게이트웨이 및 해당 데이터 처리 요금을 우회하도록 네트워크를 구성할 수 있습니다.

DataSync VPC 서비스 엔드포인트에서 Direct Connect 사용

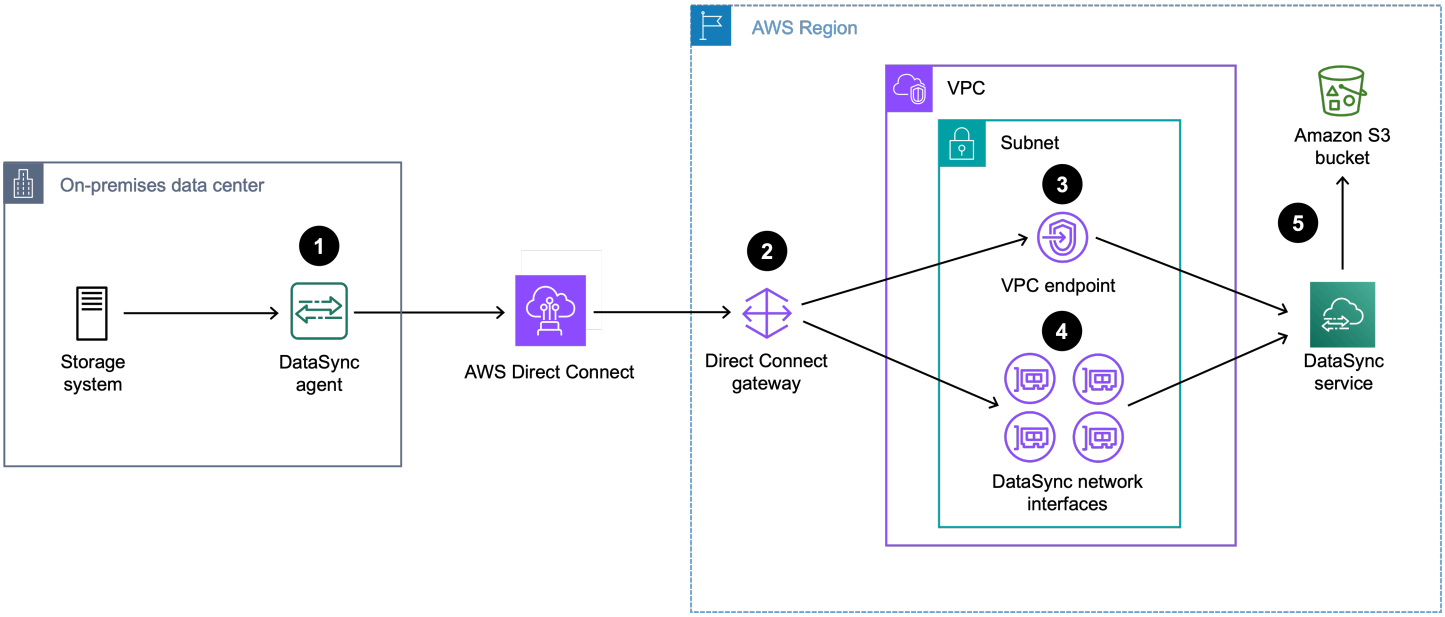
DataSync 에이전트가 VPC 서비스 엔드포인트를 사용하는 경우 VPC에 연결하려면 Direct Connect 게이트웨이가 필요합니다.

목차

- VPC 엔드포인트 및 S3 대상을 사용하는 Direct Connect 아키텍처
- 동일한 서브넷에 VPC 엔드포인트와 파일 시스템 대상이 있는 Direct Connect 아키텍처
- 서로 다른 서브넷에 VPC 엔드포인트 및 파일 시스템 대상이 있는 Direct Connect 아키텍처

VPC 엔드포인트 및 S3 대상을 사용하는 Direct Connect 아키텍처

다음 Direct Connect 아키텍처는 온프레미스 스토리지 시스템에서 S3 버킷으로의 DataSync 전송을 보여줍니다.



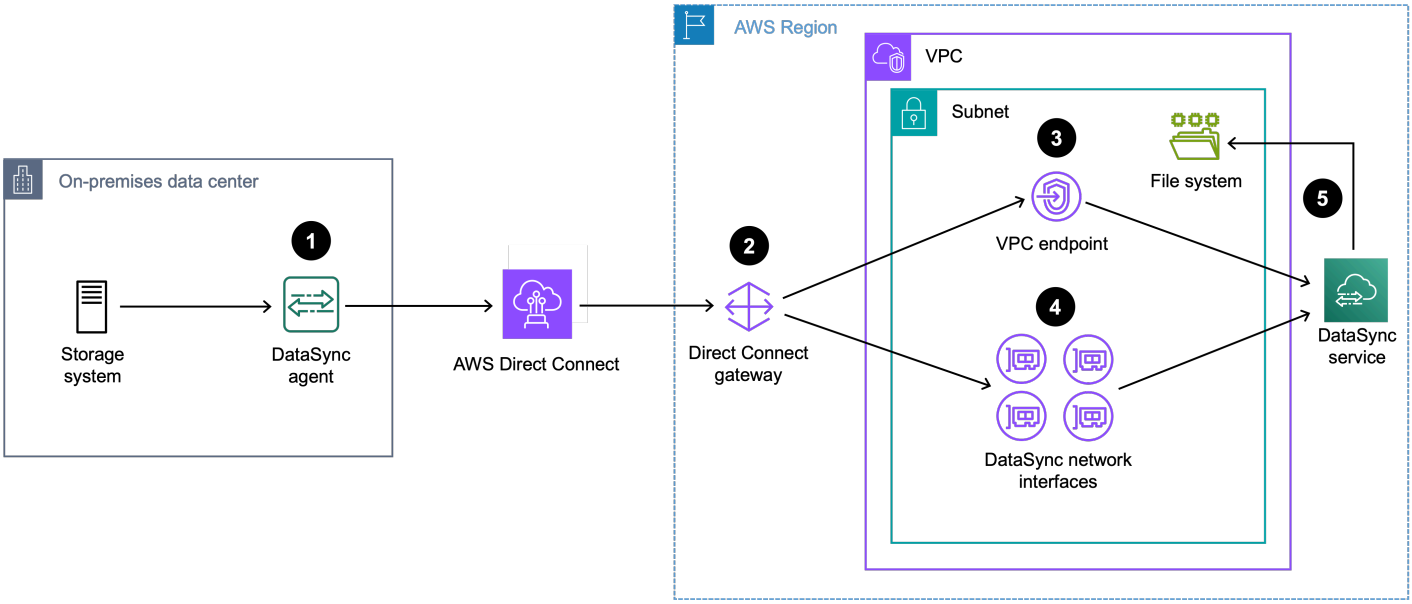
1. DataSync 에이전트는 온프레미스 스토리지 시스템(소스 위치)에서 Direct Connect 연결로 DataSync 트래픽을 라우팅합니다.
2. DataSync 트래픽은 전송에 사용되는 Direct Connect 게이트웨이로 라우팅됩니다. 이를 설정하려면 다음을 수행해야 합니다.
   a. Direct Connect 게이트웨이를 VPC의 가상 프라이빗 게이트웨이와 연결합니다. 이는 DataSync VPC 엔드포인트가 위치하고 DataSync 작업이 네트워크 인터페이스를 생성하는 VPC입니다.
   b. 이 VPC를 Direct Connect 게이트웨이에 연결하는 프라이빗 가상 인터페이스를 생성합니다.
3. DataSync 트래픽(컨트롤 플레인)은 DataSync VPC 엔드포인트를 통해 라우팅됩니다.

4. DataSync 트래픽(데이터 플레인)은 DataSync 에이전트를 생성할 때 지정하는 서브넷의 DataSync 네트워크 인터페이스를 통해 라우팅됩니다.
5. DataSync 트래픽은 DataSync 서비스를 통해 S3 버킷(대상 위치)으로 라우팅됩니다.

동일한 서브넷에 VPC 엔드포인트와 파일 시스템 대상이 있는 Direct Connect 아키텍처

Amazon EFS 또는 Amazon FSx 파일 시스템으로 또는 이러한 파일 시스템에서 전송할 때 파일 시스템과 DataSync VPC 엔드포인트가 동일한 서브넷에 있을 수 있습니다.

다음 Direct Connect 아키텍처는 온프레미스 스토리지 시스템에서 Amazon EFS 또는 Amazon FSx 파일 시스템으로의 DataSync 전송을 보여줍니다.



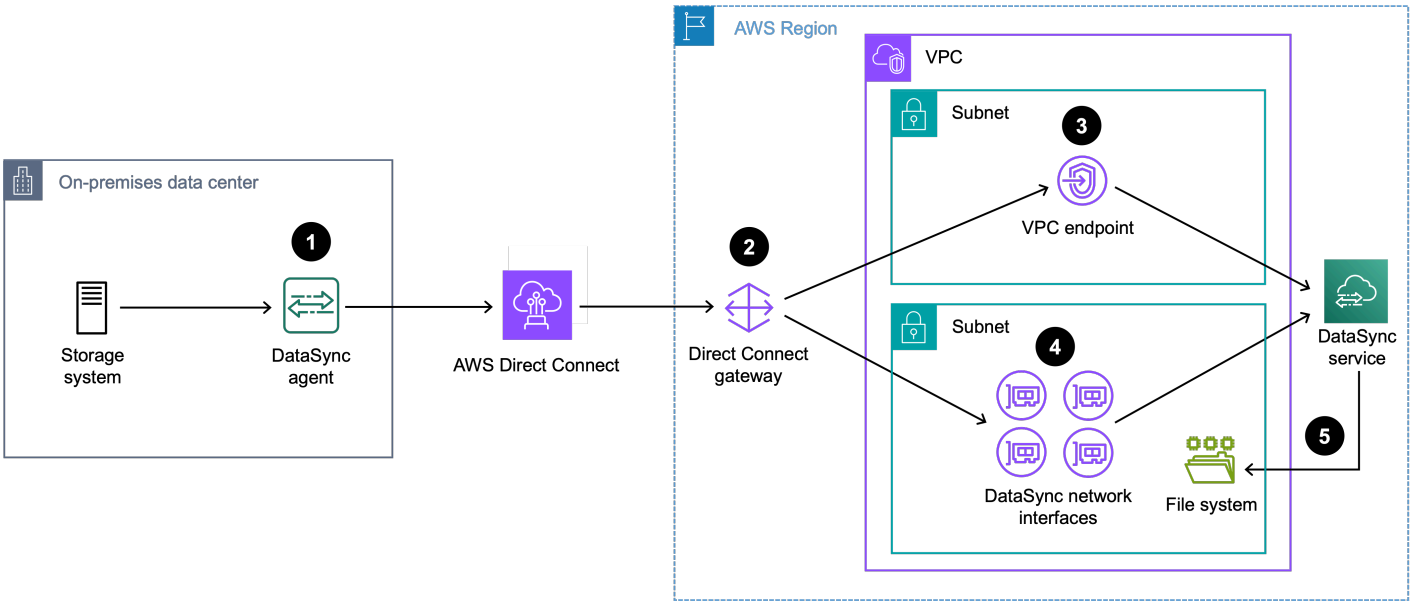
1. DataSync 에이전트는 온프레미스 스토리지 시스템(소스 위치)에서 Direct Connect 연결로 DataSync 트래픽을 라우팅합니다.
2. DataSync 트래픽은 전송에 사용되는 Direct Connect 게이트웨이로 라우팅됩니다. 이를 설정하려면 다음을 수행해야 합니다.
   a. Direct Connect 게이트웨이를 VPC의 가상 프라이빗 게이트웨이와 연결합니다. 이는 DataSync VPC 엔드포인트가 위치하고 DataSync 작업이 파일 시스템(대상 위치)에 대한 네트워크 인터페이스를 생성하는 VPC입니다.
   b. 이 VPC를 Direct Connect 게이트웨이에 연결하는 프라이빗 가상 인터페이스를 생성합니다.
3. DataSync 트래픽(컨트롤 플레인)은 DataSync VPC 엔드포인트를 통해 라우팅됩니다.
4. DataSync 트래픽(데이터 플레인)은 파일 시스템의 서브넷에 있는 DataSync 네트워크 인터페이스를 통해 라우팅됩니다. 이는 DataSync VPC 엔드포인트가 있는 서브넷과 동일합니다.

5. DataSync 트래픽은 DataSync 서비스를 통해 파일 시스템(대상 위치)으로 라우팅됩니다.

서로 다른 서브넷에 VPC 엔드포인트 및 파일 시스템 대상이 있는 Direct Connect 아키텍처

Amazon EFS 또는 Amazon FSx 파일 시스템으로 또는 이러한 파일 시스템에서 전송할 때 파일 시스템과 DataSync VPC 엔드포인트가 서로 다른 서브넷에 있을 수 있습니다.

다음 Direct Connect 아키텍처는 온프레미스 스토리지 시스템에서 Amazon EFS 또는 Amazon FSx 파일 시스템으로의 DataSync 전송을 보여줍니다.



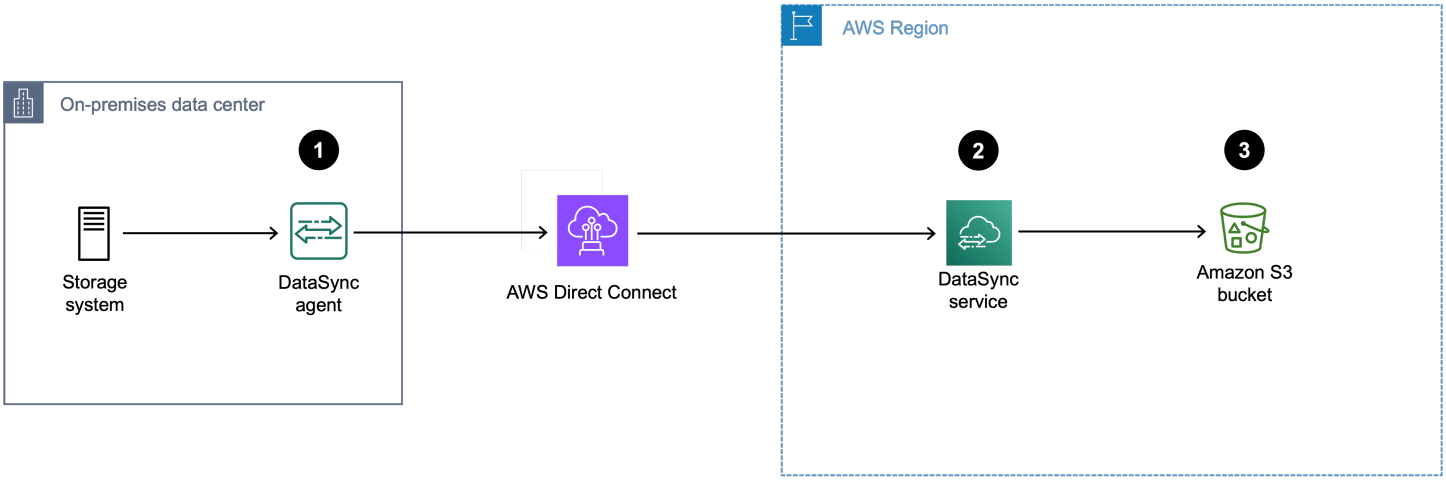
1. DataSync 에이전트는 온프레미스 스토리지 시스템(소스 위치)에서 Direct Connect 연결로 DataSync 트래픽을 라우팅합니다.
2. DataSync 트래픽은 전송에 사용되는 Direct Connect 게이트웨이로 라우팅됩니다. 이를 설정하려면 다음을 수행해야 합니다.
   a. Direct Connect 게이트웨이를 VPC의 가상 프라이빗 게이트웨이와 연결합니다. 이는 DataSync VPC 엔드포인트가 위치하고 DataSync 작업이 파일 시스템(대상 위치)에 대한 네트워크 인터페이스를 생성하는 VPC입니다.
   b. 이 VPC를 Direct Connect 게이트웨이에 연결하는 프라이빗 가상 인터페이스를 생성합니다.
3. DataSync 트래픽(컨트롤 플레인)은 DataSync VPC 엔드포인트를 통해 라우팅됩니다.
4. DataSync 트래픽(데이터 플레인)은 파일 시스템의 서브넷에 있는 DataSync 네트워크 인터페이스를 통해 라우팅됩니다. 이는 DataSync VPC 엔드포인트가 있는 서브넷과는 다릅니다.
5. DataSync 트래픽은 DataSync 서비스를 통해 파일 시스템(대상 위치)으로 라우팅됩니다.

DataSync 퍼블릭 또는 FIPS 서비스 엔드포인트에서 Direct Connect 사용

DataSync 에이전트가 퍼블릭 또는 Federal Information Processing Standard(FIPS) 서비스 엔드포인트를 사용하는 경우 퍼블릭 가상 인터페이스를 사용하여 Direct Connect 연결을 통해 데이터 전송 트래픽을 라우팅할 수 있습니다.

Direct Connect는 기본적으로 모든 로컬 및 원격 AWS 리전 접두사를 알리지만 BGP 커뮤니티 태그를 사용하여 퍼블릭 가상 인터페이스에서 트래픽의 범위(리전 또는 글로벌) 및 라우팅 기본 설정을 제어할 수 있습니다. DataSync 에이전트를 생성하려면 하나 이상의 퍼블릭 접두사를 알려야 합니다.

다음 Direct Connect 아키텍처는 퍼블릭 또는 FIPS 엔드포인트를 통해 온프레미스 스토리지 시스템에서 S3 버킷으로의 DataSync 전송을 보여줍니다.



1. DataSync 에이전트는 온프레미스 스토리지 시스템(소스 위치)에서 Direct Connect 연결로 DataSync 트래픽을 라우팅합니다.
2. DataSync 트래픽은 퍼블릭 가상 인터페이스를 통해 DataSync 서비스로 라우팅됩니다.
3. DataSync 트래픽이 S3 버킷(대상 위치)로 라우팅됩니다.

다음 단계

DataSync 에이전트가 필요하고 아직 생성하지 않은 경우 에이전트를 배포하고 에이전트의 서비스 엔드포인트를 선택한 다음 에이전트를 활성화합니다.

에이전트를 생성한 후에는 DataSync에 대한 네트워크를 구성할 수 있습니다.

여러 NICs에 대해 AWS DataSync 에이전트 구성

여러 네트워크 어댑터(NICs)를 사용하도록 AWS DataSync 에이전트를 구성하는 경우 둘 이상의 IP 주소로 에이전트에 액세스할 수 있습니다. 이 방법은 다음과 같은 상황에서 사용할 수 있습니다.

- 처리량 극대화 – 네트워크 어댑터에 병목 현상이 발생하는 경우, 에이전트에 대한 처리량을 극대화하고 싶은 경우가 있습니다.
- 네트워크 격리 - 네트워크 파일 시스템(NFS), 서버 메시지 블록(SMB), Hadoop 분산 파일 시스템(HDFS) 또는 오브젝트 스토리지 서버가 보안상의 이유로 인터넷 연결이 불가능한 가상 LAN(VLAN)에 있을 수 있습니다.

일반적인 다중 어댑터 사용 사례에서는 에이전트가 통신하는 경로 AWS (기본 에이전트)로 어댑터 하나가 구성됩니다. 이 어댑터 한 개를 제외하고 NFS, SMB, HDFS 또는 자체 관리형 객체 스토리지 위치는 연결되는 어댑터와 동일한 서브넷에 있어야 합니다.

그렇지 않은 경우, 원하는 NFS, SMB, HDFS 또는 객체 스토리지 위치와의 통신이 불가능할 수 있습니다. 경우에 따라 통신에 사용되는 동일한 어댑터에서 NFS, SMB, HDFS 또는 객체 스토리지 위치를 구성할 수 있습니다 AWS. 이러한 경우 해당 서버의 NFS, SMB, HDFS 또는 객체 스토리지 트래픽과 AWS 트래픽은 동일한 어댑터를 통해 흐릅니다.

경우에 따라 AWS DataSync 콘솔에 연결하도록 어댑터 하나를 구성한 다음 두 번째 어댑터를 추가할 수 있습니다. 이 경우, DataSync가 선호하는 경로로 두 번째 어댑터가 사용되도록 자동으로 라우팅 테이블을 구성합니다.

를 사용하여 데이터 전송 AWS DataSync

를 사용하면 온프레미스 AWS DataSync, 내부 AWS또는 다른 클라우드에 있는 스토리지와 데이터를 주고받을 수 있습니다.

DataSync 전송을 설정하려면 일반적으로 다음 단계가 필요합니다.

1. DataSync가 전송을 지원하는지 확인합니다.
2. 전송에 DataSync 에이전트가 필요한 경우 스토리지 시스템 중 하나에 최대한 가깝게 에이전트를 배포하고 활성화합니다.

   예를 들어 온프레미스 Network File System(NFS) 파일 서버에서 전송하는 경우 해당 파일 서버에 최대한 가깝게 에이전트를 배포합니다.
3. DataSync에 스토리지 시스템 액세스 권한을 제공합니다.

   DataSync에는 스토리지에서 읽거나 쓸 수 있는 권한이 필요합니다(스토리지가 소스인지 대상 위치인지에 따라 다름). 예를 들어 DataSync에 NFS 파일 서버 액세스 권한을 제공하는 방법을 알아봅니다.
4. 스토리지 시스템과 DataSync 간의 트래픽에 대해 네트워크를 연결합니다.
5. DataSync 콘솔, AWS CLI또는 DataSync API를 사용하여 소스 스토리지 시스템의 위치를 생성합니다.

   예를 들어 NFS 위치 또는 Amazon S3 위치를 생성하는 방법을 알아봅니다.
6. 3~5단계를 반복하여 전송의 대상 위치를 생성합니다.
7. 소스 및 대상 위치가 포함된 DataSync 전송 작업을 생성하고 시작합니다.

주제

- 데이터를 어디로 전송할 수 있나요 AWS DataSync?
- 를 사용하여 온프레미스 스토리지로 또는 온프레미스 스토리지에서 전송 AWS DataSync
- 를 사용하여 AWS 스토리지로 또는 스토리지에서 전송 AWS DataSync
- 를 사용하여 다른 클라우드 스토리지로 또는 다른 클라우드 스토리지에서 전송 AWS DataSync
- 사용자 데이터 전송을 위한 작업 생성
- 데이터 전송 작업 시작

데이터를 어디로 전송할 수 있나요 AWS DataSync?

를 사용하여 데이터를 전송할 수 있는 위치는 다음 요인에 AWS DataSync 따라 달라집니다.

- 전송의 출처 및 대상 위치
- 위치가 다른 경우 AWS 계정
- 위치가 다른 경우 AWS 리전
- 가 기본 모드 또는 향상된 모드를 사용하는 경우

동일한에서 지원되는 전송 AWS 계정

DataSync는 동일한 AWS 계정과 연결된 다음 스토리지 리소스 간의 전송을 지원합니다.

소스	Destination	에이전트가 필요합니까?	지원되는 작업 모드
• NFS • SMB	• Amazon S3	예	기본, 향상된
• NFS • SMB	• Amazon EFS • Amazon FSx	예	기본 전용
• HDFS • 객체 스토리지	• Amazon S3 • Amazon EFS • Amazon FSx	예	기본 전용
• 기타 클라우드 스토리지	• Amazon S3	기본 모드에만 해당	기본, 향상된
• 기타 클라우드 스토리지	• Amazon EFS • Amazon FSx	예	기본 전용
• Amazon S3	• Amazon S3	아니요	기본, 향상된
• Amazon S3	• Amazon EFS • Amazon FSx	아니요	기본 전용

소스	Destination	에이전트가 필요합니까?	지원되는 작업 모드
• Amazon S3	• NFS • SMB	예	기본, 향상된
• Amazon S3	• HDFS • 객체 스토리지	예	기본 전용
• Amazon S3	• 기타 클라우드 스토리지	기본 모드에만 해당	기본, 향상된
• Amazon EFS • Amazon FSx	• NFS • SMB	예	기본 전용
• Amazon EFS • Amazon FSx	• HDFS • 객체 스토리지	예	기본 전용
• Amazon EFS • Amazon FSx	• 기타 클라우드 스토리지	예	기본 전용
• Amazon EFS • Amazon FSx	• Amazon S3	아니요	기본 전용
• Amazon EFS • Amazon FSx	• Amazon EFS • Amazon FSx	아니요	기본 전용
• S3 on Outposts	• S3(in AWS 리전)	예	기본 전용
• Amazon S3(AWS 리전)	• S3 on Outposts	예	기본 전용

에서 지원되는 전송 AWS 계정

DataSync는 서로 다른 AWS 계정과 연결된 스토리지 리소스 간의 일부 전송을 지원합니다.

소스	Destination	에이전트가 필요합니까?	지원되는 작업 모드
• NFS • SMB	• Amazon S3	예	기본, 향상된
• HDFS • 객체 스토리지	• Amazon S3	예	기본 전용
• Amazon S3	• Amazon S3	아니요	기본, 향상된
• Amazon S3	• Amazon EFS • Amazon FSx	아니요	기본 전용
• Amazon S3	• NFS • SMB	예	기본, 향상된
• Amazon S3	• HDFS • 객체 스토리지	예	기본 전용
• Amazon EFS • Amazon FSx	• Amazon S3	아니요	기본 전용
• Amazon EFS[1] • Amazon FSx for OpenZFS[1] • Amazon FSx for Windows File Server[2] • Amazon FSx for NetApp ONTAP[3]	• Amazon EFS • Amazon FSx	예(NFS/SMB 위치로 사용되는 경우)	기본 전용

[1] NFS 위치로 구성됨.

[2] SMB 위치로 구성됨.

[3] NFS 또는 SMB 위치로 구성됩니다.

동일한에서 지원되는 전송 AWS 리전

동일한 AWS 리전 내에서 데이터를 전송할 때는 제한이 없습니다(옵트인 리전 포함). 자세한 내용은 AWS 리전 DataSync 지원을 참조하십시오.

간 지원되는 전송 AWS 리전

DataSync에서 지원하는AWS 리전 간에 데이터를 전송할 때 다음 사항에 유의하세요.

- 서로 다른의 AWS 스토리지 서비스 간에 전송할 때는 두 위치 중 AWS 리전하나가 DataSync를 사용하는 리전에 있어야 합니다.
- NFS, SMB, HDFS 또는 객체 스토리지 위치가 있는 리전에서는 전송할 수 없습니다. 이러한 상황에서는 두 전송 위치가 모두 DataSync 에이전트를 활성화한 리전과 동일한 리전에 있어야 합니다.
- AWS GovCloud (US) 리전을 사용하면 다음을 수행할 수 있습니다.
  - AWS GovCloud(미국 동부) 리전과 AWS GovCloud(미국 서부) 리전 간에 전송합니다.
  - 리전과 미국 동부(버지니아 북부) AWS 리전와 같은 상용 AWS GovCloud (US) 간 전송. Amazon EFS 또는 Amazon FSx 파일 시스템 간에 전송하는 경우 이러한 유형의 전송에는 에이전트가 필요합니다.

> **Important**
>
> 사이에 전송된 데이터에 대해 비용을 지불합니다 AWS 리전. 이 전송은 원본 리전에서 대상 리전으로의 데이터 전송으로 요금이 청구됩니다. 자세한 내용은 AWS DataSync 요금을 참조하세요.

전송에 DataSync 에이전트가 필요한지 여부 확인

전송 시나리오에 따라 DataSync 에이전트가 필요할 수 있습니다. 자세한 내용은 AWS DataSync 에이전트가 필요합니까? 섹션을 참조하세요.

를 사용하여 온프레미스 스토리지로 또는 온프레미스 스토리지에서 전송 AWS DataSync

를 사용하면 여러 온프레미스 또는 자체 관리형 스토리지 시스템과 다음 AWS 스토리지 서비스 간에 파일과 객체를 전송할 AWS DataSync수 있습니다.

- Amazon S3
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP

주제

- NFS 파일 서버를 사용하여 AWS DataSync 전송 구성
- SMB 파일 서버를 사용하여 AWS DataSync 전송 구성
- HDFS 클러스터를 사용하여 AWS DataSync 전송 구성
- 객체 스토리지 시스템을 사용하는 DataSync 전송 구성

NFS 파일 서버를 사용하여 AWS DataSync 전송 구성

를 사용하면 NFS(Network File System) 파일 서버와 다음 AWS 스토리지 서비스 간에 데이터를 전송할 AWS DataSync수 있습니다. 지원되는 스토리지 서비스는 아래와 같이 작업 모드에 따라 달라집니다.

기본 모드	확장 모드
• Amazon S3 • Amazon EFS • Amazon FSx for Windows File Server • Amazon FSx for Lustre • Amazon FSx for OpenZFS • Amazon FSx for NetApp ONTAP	• Amazon S3

이러한 종류의 전송을 설정하려면 NFS 파일 서버의 위치를 생성해야 합니다. 이 위치를 전송의 소스 또는 대상으로 사용할 수 있습니다.

DataSync에 NFS 파일 서버 액세스 권한 제공

DataSync에서 NFS 파일 서버에 액세스하려면 DataSync 에이전트가 필요합니다. 에이전트는 NFS 프로토콜을 사용하여 파일 서버에 내보내기를 마운트합니다. 원하는 작업 모드에 해당하는 에이전트를 사용해야 합니다.

주제

- NFS 내보내기 구성
- 지원되는 NFS 버전

NFS 내보내기 구성

전송을 위해 DataSync에서 필요한 내보내기는 NFS 파일 서버가 소스 위치인지 대상 위치인지와 파일 서버 권한이 구성된 방식에 따라 달라집니다.

파일 서버가 소스 위치인 경우 DataSync는 파일과 폴더를 읽고 탐색하기만 하면 됩니다. 대상 위치인 경우 DataSync에서 위치에 쓰기를 수행하고 복사하려는 파일 및 폴더에 소유권, 권한 및 기타 메타데이터를 설정할 수 있는 루트 액세스 권한이 필요합니다. `no_root_squash` 옵션을 사용하여 내보내기에 루트 액세스를 허용할 수 있습니다.

다음 예제는 DataSync에 대한 액세스를 제공하는 NFS 내보내기를 구성하는 방법을 설명합니다.

NFS 파일 서버가 소스 위치인 경우(루트 액세스)

DataSync 읽기 전용 권한(`ro`) 및 루트 액세스(`no_root_squash`)를 제공하는 다음 명령을 사용하여 내보내기를 구성합니다.

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

NFS 파일 서버가 대상 위치인 경우

DataSync 쓰기 전용 권한(`rw`) 및 루트 액세스(`no_root_squash`)를 제공하는 다음 명령을 사용하여 내보내기를 구성합니다.

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

NFS 파일 서버가 소스 위치인 경우(루트 액세스 아님)

내보내기에 대한 DataSync 읽기 전용 권한을 제공하는 것으로 알고 있는 POSIX 사용자 ID(UID) 및 GID(그룹 ID)를 지정하는 다음 명령을 사용하여 내보내기를 구성합니다.

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

지원되는 NFS 버전

기본적으로 DataSync는 NFS 버전 4.1을 사용합니다. DataSync는 NFS 4.0 및 3.x도 지원합니다.

NFS 전송을 위한 네트워크 구성

DataSync 전송의 경우 몇 가지 네트워크 연결에 대한 트래픽을 구성해야 합니다.

1. DataSync 에이전트에서 NFS 파일 서버로 다음 포트의 트래픽을 허용합니다.

   - NFS 버전 4.1 및 4.0-TCP 포트 2049
   - NFS 버전 3.x-TCP 포트 111 및 2049

   네트워크의 다른 NFS 클라이언트는 데이터 전송에 사용하는 NFS 내보내기를 마운트할 수 있어야 합니다. 내보내기는 Kerberos 인증 없이도 액세스할 수 있어야 합니다.
2. 서비스 엔드포인트 연결(예: VPC, 퍼블릭 또는 FIPS 엔드포인트)에 대한 트래픽을 구성합니다.
3. DataSync 서비스에서 전송 중인 AWS 스토리지 서비스로의 트래픽을 허용합니다.

NFS 전송 위치 생성

시작하기 전에 다음 사항에 유의하세요.

- 데이터를 전송할 NFS 파일 서버가 필요합니다.
- 파일 서버에 액세스할 수 있는 DataSync 에이전트가 필요합니다.
- DataSync는 NFS 버전 4 액세스 제어 목록(ACL) 복사를 지원하지 않습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 네트워크 파일 시스템(NFS)을 선택합니다.
4. 에이전트에서 NFS 파일 서버에 연결할 수 있는 DataSync 에이전트를 선택합니다.

   2개 이상의 에이전트를 선택할 수 있습니다. 자세한 설명은 여러 DataSync 에이전트 사용섹션을 참조하세요.

5. NFS 서버에는 DataSync 에이전트가 연결하는 NFS 파일 서버의 도메인 이름 시스템(DNS) 이름 또는 IP 주소를 입력합니다.
6. 마운트 경로에는 DataSync에서 마운트할 NFS 내보내기 경로를 입력합니다.

   이 경로(또는 경로의 하위 디렉터리)는 DataSync가 데이터를 전송하고 전송 받는 곳입니다. 자세한 설명은 NFS 내보내기 구성섹션을 참조하세요.
7. (선택 사항) 추가 설정을 확장하고 DataSync가 파일 서버에 액세스할 때 사용할 특정 NFS 버전을 선택합니다.

   자세한 설명은 지원되는 NFS 버전섹션을 참조하세요.
8. (선택 사항) 태그 추가를 선택하여 NFS 위치에 태그를 지정합니다.

   태그는 위치를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.
9. 위치 생성을 선택합니다.

사용 AWS CLI

- 다음 명령을 사용하여 NFS 위치를 생성합니다.

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

위치 생성에 대한 자세한 정보는 DataSync에 NFS 파일 서버 액세스 권한 제공(을)를 참조하세요.

NFS 위치에서 읽는 데 사용하는 NFS 버전을 DataSync가 자동으로 선택합니다. NFS 버전을 지정하려면 NfsMountOptions API 작업에서 선택적 `Version` 파라미터를 사용합니다.

이들 명령은 다음과 같은 Amazon 리소스 이름(ARN)과 비슷한 NFS 위치의 ARN을 반환합니다.

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

디렉터리를 탑재할 수 있는지 확인하려면 에이전트와 동일한 네트워크 구성을 가진 컴퓨터에 연결하여 다음 명령을 실행하세요.

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

다음은 명령의 예제입니다.

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

SMB 파일 서버를 사용하여 AWS DataSync 전송 구성

를 사용하면 SMB(Server Message Block) 파일 서버와 다음 AWS 스토리지 서비스 간에 데이터를 전송할 AWS DataSync수 있습니다. 지원되는 스토리지 서비스는 아래와 같이 작업 모드에 따라 달라집니다.

기본 모드	확장 모드
• Amazon S3 • Amazon EFS • Amazon FSx for Windows File Server • Amazon FSx for Lustre • Amazon FSx for OpenZFS • Amazon FSx for NetApp ONTAP	• Amazon S3

이러한 종류의 전송을 설정하려면 SMB 파일 서버의 위치를 생성해야 합니다. 이를 전송의 소스 또는 대상으로 사용할 수 있습니다. 원하는 작업 모드에 해당하는 에이전트를 사용해야 합니다.

DataSync에 SMB 파일 서버 액세스 권한 제공

DataSync는 SMB 프로토콜을 사용하여 파일 서버에 연결하고 NTLM 또는 Kerberos로 인증할 수 있습니다.

주제

- 지원되는 SMB 버전
- NTLM 인증 사용

- Kerberos 인증 사용
- 필수 권한
- DFS 네임스페이스

지원되는 SMB 버전

기본적으로 DataSync는 SMB 파일 서버와의 협상을 기반으로 SMB 프로토콜 버전을 자동으로 선택합니다.

특정 SMB 버전을 사용하도록 DataSync를 구성할 수도 있지만 DataSync가 SMB 파일 서버와 자동으로 협상하는 데 문제가 있는 경우에만 이렇게 하는 것이 좋습니다. DataSync는 SMB 버전 1.0 이상을 지원합니다. 보안상의 이유로 SMB 버전 3.0.2 이상을 사용하는 것이 좋습니다. SMB 1.0과 같은 이전 버전에는 알려진 보안 취약성이 포함되어 있어, 공격자가 데이터를 손상시키기 위해 이를 악용할 수 있습니다.

DataSync 콘솔 및 API의 옵션 목록은 다음 표를 참조하세요.

콘솔 옵션	API 옵션	설명
자동	`AUTOMATIC`	DataSync와 SMB 파일 서버는 2.1과 3.1.1 사이에서 상호 지원하는 SMB의 가장 높은 버전을 협상합니다. 이는 기본값이며 권장 옵션입니다. 대신 파일 서버에서 지원하지 않는 특정 버전을 선택하면 `Operation Not Supported` 오류가 발생할 수 있습니다.
SMB 3.0.2	`SMB3`	프로토콜 협상을 SMB 버전 3.0.2로만 제한합니다.
SMB 2.1	`SMB2`	프로토콜 협상을 SMB 버전 2.1로만 제한합니다.
SMB 2.0	`SMB2_0`	프로토콜 협상을 SMB 버전 2.0으로만 제한합니다.
SMB 1.0	`SMB1`	프로토콜 협상을 SMB 버전 1.0으로만 제한합니다.

NTLM 인증 사용

NTLM 인증을 사용하려면 사용자 이름과 암호를 제공하여 DataSync가 전송을 주고 받는 SMB 파일 서버에 액세스하도록 허용합니다. 해당 사용자는 파일 서버의 로컬 사용자이거나 Microsoft Active Directory의 도메인 사용자일 수 있습니다.

Kerberos 인증 사용

Kerberos 인증을 사용하려면 Kerberos 보안 주체, Kerberos 키 테이블(키 탭) 파일, Kerberos 구성 파일을 제공하여 DataSync가 전송을 주고 받는 SMB 파일 서버에 액세스하도록 허용합니다.

주제

- 사전 조건
- Kerberos에 대한 DataSync 구성 옵션

사전 조건

몇 가지 Kerberos 아티팩트를 생성하고 네트워크를 구성하면 DataSync가 SMB 파일 서버에 액세스할 수 있습니다.

- ktpass 또는 kutil 유틸리티를 사용하여 Kerberos 키탭 파일을 생성합니다.

  다음 예시에서는 `ktpass`를 사용하여 키탭 파일을 생성합니다. 지정한 Kerberos 영역(`MYDOMAIN.ORG`)은 대문자여야 합니다.

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

- 간소화된 버전의 Kerberos 구성 파일(`krb5.conf`)을 준비합니다. 영역, 도메인 관리자 서버의 위치, Kerberos 영역에 대한 호스트 이름 매핑에 대한 정보를 포함합니다.

  `krb5.conf` 콘텐츠가 영역 및 도메인 영역 이름에 대한 올바른 대/소문자 형식으로 혼합되어 있는지 확인합니다. 예제:

  ```
  [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
```

- 네트워크 구성에서 Kerberos 키 분배 센터(KDC) 서버 포트가 열려 있는지 확인합니다. KDC 포트는 일반적으로 TCP 포트 88입니다.

Kerberos에 대한 DataSync 구성 옵션

Kerberos를 사용하는 SMB 위치를 생성할 때 다음 옵션을 구성합니다.

콘솔 옵션	API 옵션	설명
SMB 서버	`ServerHostName`	DataSync 에이전트가 탑재할 SMB 파일 서버의 도메인 이름입니다. Kerberos에서는 파일 서버의 IP 주소를 지정할 수 없습니다.
Kerberos 보안 주체	`KerberosPrincipal`	Kerberos 영역의 자격 증명으로, SMB 파일 서버의 파일, 폴더, 파일 메타데이터에 액세스할 권한을 가집니다. Kerberos 보안 주체는 `HOST/kerberosuser@MYDOMAIN.ORG` 처럼 보일 수 있습니다. 보안 주체 이름은 대/소문자를 구분합니다.
키탭 파일	`KerberosKeytab`	Kerberos 보안 주체와 암호화 키 간의 매핑을 포함하는 Kerberos 키 테이블(키탭) 파일입니다.
Kerberos 구성 파일	`KerberosKrbConf`	Kerberos 영역 구성을 정의하는 `krb5.conf` 파일입니다.

콘솔 옵션	API 옵션	설명
DNS IP 주소(선택 사항)	`DnsIpAddresses`	SMB 파일 서버가 속한 DNS 서버의 IPv4 주소입니다. 환경에 여러 도메인이 있는 경우 이를 구성하면 DataSync가 올바른 SMB 파일 서버에 연결되도록 할 수 있습니다.

필수 권한

DataSync에 SMB 파일 서버의 파일, 폴더, 파일 메타데이터를 탑재하고 액세스하기 위한 필수 권한을 제공해야 합니다.

Active Directory에 자격 증명을 제공하는 경우, 이는 다음 사용자 권한 중 하나 또는 둘 다(DataSync가 복사할 메타데이터에 따라 다름)를 가진 Active Directory 그룹의 구성원이어야 합니다.

사용자 권한	설명
파일 및 디렉터리 복원(`SE_RESTORE_NAME `)	DataSync가 객체 소유권, 권한, 파일 메타데이터, NTFS 임의 액세스 목록(DACL)을 복사하도록 허용합니다. 이 사용자 권한은 일반적으로 도메인 관리자 및 백업 운영자 그룹(둘 다 기본 Active Directory 그룹)의 멤버에게 부여됩니다.
감사 및 보안 로그 관리(`SE_SECURITY_NAME `)	DataSync가 NTFS 시스템 액세스 제어 목록(SACL)을 복사하도록 허용합니다. 이 사용자 권한은 일반적으로 도메인 관리자 그룹의 멤버에게 부여됩니다.

Windows ACL을 복사하려는 경우와 SMB 파일 서버 및 SMB를 사용하는 다른 스토리지 시스템(예: Amazon FSx for Windows File Server 또는 FSx for ONTAP) 간에 전송하는 경우, DataSync에 제공하

는 자격 증명은 같은 Active Directory 도메인에 속하거나 도메인 간에 Active Directory 신뢰 관계가 있어야 합니다.

DFS 네임스페이스

DataSync는 Microsoft 분산 파일 시스템(DFS) 네임스페이스를 지원하지 않습니다. DataSync 위치를 생성할 때 기본 파일 서버 또는 공유를 지정하는 것이 좋습니다.

SMB 전송 위치 생성

시작하려면 데이터를 전송할 SMB 파일 서버가 필요합니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. Location type(위치 유형)에서 Server Message Block (SMB)(SMB(Server Message Block))을 선택합니다.

   나중에 이 위치를 소스 또는 대상 주소로서 구성합니다.
4. 에이전트에서 SMB 파일 서버에 연결할 수 있는 DataSync 에이전트를 선택합니다.

   2개 이상의 에이전트를 선택할 수 있습니다. 자세한 내용은 여러 DataSync 에이전트 사용 단원을 참조하십시오.
5. SMB 서버에서 DataSync 에이전트가 탑재할 SMB 파일 서버의 도메인 이름 또는 IP 주소를 입력합니다.

   이 설정에서는 다음 사항에 유의하세요.

   - IP 버전 6(IPv6) 주소는 지정할 수 없습니다.
   - Kerberos 인증을 사용하는 경우 도메인 이름을 지정해야 합니다.
6. 공유 이름에는 DataSync가 데이터를 읽거나 쓸 SMB 파일 서버에서 내보낸 공유의 이름을 입력합니다.

   공유 경로에 하위 디렉토리(예: `/path/to/subdirectory`)를 포함할 수 있습니다. 네트워크의 다른 SMB 클라이언트도 이 경로를 마운트할 수 있는지 확인하세요.

   하위 디렉터리의 모든 데이터를 복사하려면 DataSync가 SMB 공유를 마운트하고 모든 데이터에 액세스할 수 있어야 합니다. 자세한 설명은 필수 권한섹션을 참조하세요.

7. (선택 사항) 추가 설정을 확장하고 DataSync가 파일 서버에 액세스할 때 사용할 SMB 버전을 선택합니다.

   기본적으로 DataSync는 SMB 파일 서버와의 협상을 기반으로 버전을 자동으로 선택합니다. 자세한 내용은 지원되는 SMB 버전 단원을 참조하세요.
8. 인증 유형에서 NTLM 또는 Kerberos를 선택합니다.
9. 선택한 인증 유형에 따라 다음 중 하나를 수행합니다.

   NTLM

   - 사용자에는 SMB 파일 서버를 마운트할 수 있고 전송과 관련된 파일 및 폴더에 액세스할 수 있는 권한을 가진 사용자 이름을 입력합니다.

     자세한 설명은 필수 권한섹션을 참조하세요.
   - 암호에는 SMB 파일 서버를 마운트할 수 있고 전송과 관련된 파일 및 폴더에 액세스할 수 있는 권한을 가진 사용자의 암호를 입력합니다.
   - (선택 사항) 도메인에는 SMB 파일 서버가 속하는 Windows 도메인 이름을 입력합니다.

     환경에 여러 도메인이 있는 경우 이 설정을 구성하면 DataSync가 올바른 SMB 파일 서버에 연결할 수 있습니다.

   Kerberos

   - Kerberos 보안 주체에서 SMB 파일 서버의 파일, 폴더, 파일 메타데이터에 액세스할 권한이 있는 보안 주체를 Kerberos 영역에 지정합니다.

     Kerberos 보안 주체는 `HOST/kerberosuser@MYDOMAIN.ORG`처럼 보일 수 있습니다.

     보안 주체 이름은 대/소문자를 구분합니다. 이 설정에 대해 지정한 보안 주체가 키탭 파일 생성에 사용하는 보안 주체와 정확히 일치하지 않으면 DataSync 작업 실행이 실패합니다.
   - Keytab 파일에서 Kerberos 보안 주체와 암호화 키 간의 매핑을 포함하는 키탭 파일을 업로드합니다.
   - Kerberos 구성 파일에서 Kerberos 영역 구성을 정의하는 `krb5.conf` 파일을 업로드합니다.
   - (선택 사항) DNS IP 주소에서 SMB 파일 서버가 속한 DNS 서버에 대해 최대 2개의 IPv4 주소를 지정합니다.

     환경에 여러 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 SMB 파일 서버에 연결되도록 할 수 있습니다.

10. (선택 사항) 태그 추가를 선택하여 SMB 위치에 태그를 지정합니다.

    태그는 위치를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

11. 위치 생성을 선택합니다.

사용 AWS CLI

다음 지침은 NTLM 또는 Kerberos 인증을 사용하여 SMB 위치를 생성하는 방법을 설명합니다.

NTLM

1. 다음 `create-location-smb`명령을 복사합니다.

```
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. `--agent-arns`에서 SMB 파일 서버에 연결할 DataSync 에이전트를 지정합니다.

   2개 이상의 에이전트를 선택할 수 있습니다. 자세한 내용은 여러 DataSync 에이전트 사용 단원을 참조하십시오.

3. `--server-hostname`에서 DataSync 에이전트가 탑재할 SMB 파일 서버의 도메인 이름 또는 IPv4 주소를 지정합니다.

4. `--subdirectory`에서 DataSync가 데이터를 읽거나 쓸 SMB 파일 서버에서 내보낸 공유 이름을 지정합니다.

   공유 경로에 하위 디렉토리(예: `/path/to/subdirectory`)를 포함할 수 있습니다. 네트워크의 다른 SMB 클라이언트도 이 경로를 마운트할 수 있는지 확인하세요.

   하위 디렉터리의 모든 데이터를 복사하려면 DataSync가 SMB 공유를 마운트하고 모든 데이터에 액세스할 수 있어야 합니다. 자세한 내용은 필수 권한 단원을 참조하십시오.

5. `--user`에서 사용자의 SMB 파일 서버를 탑재할 수 있고 전송과 관련된 파일 및 폴더에 액세스할 권한을 가진 사용자 이름을 지정합니다.

자세한 내용은 필수 권한 단원을 참조하십시오.

6. `--password`에서 사용자 SMB 파일 서버를 탑재하고 전송과 관련된 파일과 폴더에 액세스할 권한이 있는 사용자의 암호를 지정합니다.
7. (선택 사항) `--domain`에서 SMB 파일 서버가 속한 Windows 도메인 이름을 지정합니다.

   환경에 여러 도메인이 있는 경우 이 설정을 구성하면 DataSync가 올바른 SMB 파일 서버에 연결할 수 있습니다.
8. (선택 사항) DataSync가 특정 SMB 버전을 사용하도록 하려면 `--version` 옵션을 추가합니다. 자세한 내용은 지원되는 SMB 버전 단원을 참조하십시오.
9. `create-location-smb` 명령을 실행합니다.

   명령이 성공하면 생성한 위치의 ARN을 보여주는 응답을 받게 됩니다. 예제:

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

Kerberos

1. 다음 `create-location-smb`명령을 복사합니다.

```
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. `--agent-arns`에서 SMB 파일 서버에 연결할 DataSync 에이전트를 지정합니다.

   2개 이상의 에이전트를 선택할 수 있습니다. 자세한 내용은 여러 DataSync 에이전트 사용 단원을 참조하십시오.
3. `--server-hostname`에서 DataSync 에이전트가 탑재할 SMB 파일 서버의 도메인 이름을 지정합니다.

4. `--subdirectory`에서 DataSync가 데이터를 읽거나 쓸 SMB 파일 서버에서 내보낸 공유 이름을 지정합니다.

   공유 경로에 하위 디렉토리(예: `/path/to/subdirectory`)를 포함할 수 있습니다. 네트워크의 다른 SMB 클라이언트도 이 경로를 마운트할 수 있는지 확인하세요.

   하위 디렉터리의 모든 데이터를 복사하려면 DataSync가 SMB 공유를 마운트하고 모든 데이터에 액세스할 수 있어야 합니다. 자세한 내용은 필수 권한 단원을 참조하십시오.

5. Kerberos 옵션의 경우 다음을 수행합니다.

   - `--kerberos-principal`: SMB 파일 서버의 파일, 폴더, 파일 메타데이터에 액세스할 권한이 있는 보안 주체를 Kerberos 영역에 지정합니다.

     Kerberos 보안 주체는 `HOST/kerberosuser@MYDOMAIN.ORG`처럼 보일 수 있습니다.

     보안 주체 이름은 대/소문자를 구분합니다. 이 옵션에 대해 지정한 보안 주체가 키탭 파일 생성에 사용하는 보안 주체와 정확히 일치하지 않으면 DataSync 작업 실행이 실패합니다.
   - `--kerberos-keytab`: Kerberos 보안 주체와 암호화 키 간의 매핑을 포함하는 키탭 파일을 지정합니다.
   - `--kerberos-krb5-conf`: Kerberos 영역 구성을 정의하는 `krb5.conf` 파일을 지정합니다.
   - (선택 사항) `--dns-ip-addresses`: SMB 파일 서버가 속한 DNS 서버에 대해 최대 2개의 IPv4 주소를 지정합니다.

     환경에 여러 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 SMB 파일 서버에 연결되도록 할 수 있습니다.

6. (선택 사항) DataSync가 특정 SMB 버전을 사용하도록 하려면 `--version` 옵션을 추가합니다. 자세한 내용은 지원되는 SMB 버전 단원을 참조하십시오.

7. `create-location-smb` 명령을 실행합니다.

   명령이 성공하면 생성한 위치의 ARN을 보여주는 응답을 받게 됩니다. 예제:

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

HDFS 클러스터를 사용하여 AWS DataSync 전송 구성

를 사용하면 기본 모드 작업을 사용하여 하둡 분산 파일 시스템(HDFS) 클러스터와 다음 AWS 스토리지 서비스 중 하나 간에 데이터를 전송할 AWS DataSync수 있습니다.

- Amazon S3
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP

이러한 종류의 전송을 설정하려면 HDFS 클러스터의 위치를 생성해야 합니다. 이 위치를 전송의 소스 또는 대상으로 사용할 수 있습니다.

DataSync에 HDFS 클러스터 액세스 권한 제공

DataSync는 HDFS 클러스터에 연결하기 위해 HDFS 클러스터에 최대한 가깝게 배포하는 기본 모드 에이전트를 사용합니다. DataSync 에이전트는 HDFS 클라이언트 역할을 하며 클러스터의 NameNodes 및 DataNodes와 통신합니다.

전송 작업을 시작하면 DataSync는 클러스터의 파일 및 폴더 위치에 대한 NameNode 쿼리를 제기합니다. HDFS 위치가 소스 위치로 구성된 경우 DataSync는 클러스터의 DataNodes에서 파일 및 폴더 데이터를 읽고 데이터를 대상으로 복사합니다. HDFS 위치가 대상 위치로 구성된 경우 DataSync는 소스에서 클러스터의 DataNodes로 파일 및 폴더를 씁니다.

Authentication

HDFS 클러스터에 연결할 때 DataSync는 단순 인증 또는 Kerberos 인증을 지원합니다. 단순 인증을 사용하려면 HDFS 클러스터에 대한 읽기 및 쓰기 권한이 있는 사용자의 사용자 이름을 제공하세요. Kerberos 인증을 사용하려면 Kerberos 구성 파일, Kerberos 키 테이블(keytab) 파일 및 Kerberos 보안 주체를 제공하세요. Kerberos 보안 주체의 보안 인증은 제공된 keytab 파일에 있어야 합니다.

암호화(Encryption)

Kerberos 인증을 사용하는 경우 DataSync는 DataSync 에이전트와 HDFS 클러스터 간에 전송되는 데이터의 암호화를 지원합니다. HDFS 위치를 생성할 때 HDFS 클러스터의 QOP(Quality of Protection)

구성 설정을 사용하고 QOP 설정을 지정하여 데이터를 암호화합니다. QOP 구성에는 데이터 전송 보호 및 원격 프로시저 호출(RPC) 보호 설정이 포함됩니다.

DataSync는 다음과 같은 Kerberos 암호화 유형을 지원합니다.

- `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`

투명한 데이터 암호화(TDE)를 사용하여 유휴 시 암호화에 대해 HDFS 클러스터를 구성할 수도 있습니다. 단순 인증을 사용하는 경우 DataSync는 TDE 지원 클러스터를 읽고 씁니다. DataSync를 사용하여 TDE 지원 클러스터에 데이터를 복사하는 경우 먼저 HDFS 클러스터에서 암호화 영역을 구성하세요. DataSync는 암호화 영역을 생성하지 않습니다.

지원되지 않는 HDFS 기능

다음과 같은 HDFS의 기능은 현재 DataSync에서 지원되지 않습니다.

- Kerberos 인증 사용 시 투명한 데이터 암호화(TDE)
- 다중 NameNode 구성
- HTTP를 통한 Hadoop HDFS(HTTPFS)
- POSIX 액세스 제어 목록(ACL)
- HDFS 확장 속성(xatter)
- Apache HBase를 사용하는 HDFS 클러스터

HDFS 전송 위치 생성

이 위치를 DataSync 전송의 소스 또는 대상으로 사용할 수 있습니다.

시작하기 전: 다음을 수행하여 에이전트와 Hadoop 클러스터 간의 네트워크 연결을 확인합니다.

- 온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항에 나열된 TCP 포트에 대한 액세스를 테스트합니다.
- 로컬 에이전트와 Hadoop 클러스터 간의 액세스를 테스트합니다. 지침은 에이전트의 스토리지 시스템 연결 확인 섹션을 참조하세요.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 Hadoop 분산 파일 시스템(HDFS)을 선택합니다.

   나중에 이 위치를 소스 또는 대상으로 구성할 수 있습니다.
4. 에이전트에서 HDFS 클러스터에 연결할 수 있는 에이전트를 선택합니다.

   2개 이상의 에이전트를 선택할 수 있습니다. 자세한 내용은 여러 DataSync 에이전트 사용 단원을 참조하십시오.
5. NameNode에서 HDFS 클러스터의 기본 NameNode의 도메인 이름 또는 IP 주소를 입력합니다.
6. 폴더에서 DataSync가 데이터 전송에 사용하길 원하는 HDFS 클러스터의 폴더를 입력합니다.

   HDFS 위치가 소스인 경우 DataSync는 이 폴더의 파일을 대상으로 복사합니다. 위치가 대상인 경우 DataSync는 이 폴더에 파일을 씁니다.
7. 블록 크기 또는 복제 인수를 설정하려면 추가 설정을 선택합니다.

   기본 블록 크기는 128MiB입니다. 제공하는 블록 크기는 512바이트의 배수여야 합니다.

   HDFS 클러스터로 전송할 때 기본 복제 인수는 세 개의 DataNode입니다.
8. 보안 섹션에서 HDFS 클러스터에 사용되는 인증 유형을 선택합니다.

   - 단순 – 사용자에, HDFS 클러스터에서 다음 권한을 가진 사용자 이름을 지정합니다(사용 사례에 따라 다름).
     - 이 위치를 소스 위치로 사용하려는 경우 읽기 권한만 있는 사용자를 지정합니다.

- 이 위치를 대상 위치로 사용하려는 경우 읽기 권한과 쓰기 권한이 있는 사용자를 지정합니다.

  선택적으로, HDFS 클러스터의 키 관리 서버(KMS) URI를 지정합니다.

- Kerberos – HDFS 클러스터에 액세스할 수 있는 Kerberos 보안 주체를 지정합니다. 다음으로, 제공된 Kerberos 보안 주체가 포함된 KeyTab 파일을 제공합니다. 그런 다음 Kerberos 구성 파일을 제공합니다. 마지막으로 RPC 보호 및 데이터 전송 보호 드롭다운 목록에서 전송 중 암호화 보호 유형을 지정합니다.

9. (선택 사항) 태그 추가를 선택하여 HDFS 위치에 태그를 지정합니다.

   태그는 위치를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

10. 위치 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-location-hdfs`명령을 복사합니다.

```
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. `--name-nodes` 파라미터에서 HDFS 클러스터의 기본 NameNode의 호스트 이름 또는 IP 주소와 NameNode가 수신 대기 중인 TCP 포트를 지정합니다.

3. `--authentication-type` 파라미터에서 Hadoop 클러스터에 연결할 때 사용할 인증 유형을 지정합니다. `SIMPLE` 또는 `KERBEROS`를 지정할 수 있습니다.

   `SIMPLE` 인증을 사용하는 경우 `--simple-user`파라미터를 사용하여 사용자의 사용자 이름을 지정합니다. `KERBEROS` 인증을 사용하는 경우 `--kerberos-principal`, `--kerberos-keytab`, 및 `--kerberos-krb5-conf`파라미터를 사용합니다. 자세한 내용은 create-location-hdfs를 참조하세요.

4. `--agent-arns` 파라미터에서 HDFS 클러스터에 연결할 수 있는 DataSync 에이전트의 ARN을 지정합니다.

   2개 이상의 에이전트를 선택할 수 있습니다. 자세한 내용은 여러 DataSync 에이전트 사용 단원을 참조하십시오.

5. (선택 사항) `--subdirectory` 파라미터에서 DataSync가 데이터 전송에 사용할 HDFS 클러스터의 폴더를 지정합니다.

   HDFS 위치가 소스인 경우 DataSync는 이 폴더의 파일을 대상으로 복사합니다. 위치가 대상인 경우 DataSync는 이 폴더에 파일을 씁니다.

6. `create-location-hdfs` 명령을 실행합니다.

   명령이 성공하면 생성한 위치의 ARN을 보여주는 응답을 받게 됩니다. 예제:

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

객체 스토리지 시스템을 사용하는 DataSync 전송 구성

를 사용하면 기본 모드 작업을 사용하여 객체 스토리지 시스템과 다음 AWS 스토리지 서비스 중 하나 간에 데이터를 전송할 AWS DataSync수 있습니다.

- Amazon S3
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP

이러한 종류의 전송을 설정하려면 객체 스토리지 시스템의 위치를 생성해야 합니다. 이 위치를 전송의 소스 또는 대상으로 사용할 수 있습니다. 온프레미스 객체 스토리지에서 데이터를 전송하려면 기본 모드 DataSync 에이전트가 필요합니다.

사전 조건

DataSync가 연결하려면 클라우드 객체 스토리지 시스템이 다음의 Amazon S3 API 작업과 호환되어야 합니다.

- `AbortMultipartUpload`
- `CompleteMultipartUpload`

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

객체 스토리지 전송 위치 생성

시작하려면 데이터를 주고받으며 전송할 객체 스토리지 시스템이 필요합니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 객체 스토리지를 선택합니다.

   나중에 이 위치를 소스 또는 대상 주소로서 구성합니다.
4. 서버에는 객체 스토리지 서버의 도메인 이름 또는 IP 주소를 지정합니다.
5. 버킷 이름에는 전송과 관련된 객체 스토리지 버킷의 이름을 입력합니다.
6. 폴더에는 객체 접두사를 입력합니다.

   DataSync는 이 접두사가 있는 객체만 복사합니다.
7. 전송에 에이전트가 필요한 경우 에이전트 사용을 선택한 다음 DataSync 에이전트를 선택하여 객체 스토리지 시스템에 연결합니다.

일부 전송에는 에이전트가 필요하지 않습니다. 다른 시나리오에서는 둘 이상의 에이전트를 사용하는 것이 좋을 수 있습니다. 자세한 내용은 DataSync 에이전트가 필요하지 않은 상황 및 여러 DataSync 에이전트 사용 섹션을 참조하세요.

8. 객체 스토리지 서버에 대한 연결을 구성하려면 추가 설정을 확장하고 다음을 수행하세요.

   a. 서버 프로토콜에서 HTTP 또는 HTTPS를 선택합니다.

   b. 서버 포트에는 기본 포트(HTTP의 경우 80, HTTPS의 경우 443)를 사용하거나 필요한 경우 사용자 지정 포트를 지정합니다.

   c. 인증서에서 객체 스토리지 시스템이 프라이빗 또는 자체 서명된 인증 기관(CA)을 사용하는 경우 파일 선택을 선택하고 전체 인증서 체인이 있는 단일 `.pem` 파일을 지정합니다.

      인증서 체인에는 다음이 포함될 수 있습니다.

      - 객체 스토리지 시스템의 인증서
      - 모든 중간 인증서(있는 경우)
      - 서명 CA의 루트 인증서

      인증서를 `.pem` 파일로 연결할 수 있습니다(base64 인코딩 전 최대 32,768바이트). 다음 예제의 `cat` 명령은 세 개의 인증서가 포함된 *`object_storage_certificates`*`.pem` 파일을 생성합니다.

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

9. 객체 스토리지 서버가 액세스를 위해 자격 증명을 요구하는 경우 자격 증명 필요를 선택하고 버킷에 액세스하기 위한 액세스 키를 입력합니다. 그런 다음 보안 키를 직접 입력하거나 키가 포함된 AWS Secrets Manager 보안 암호를 지정합니다. 자세한 내용은 스토리지 위치에 대한 자격 증명 제공을 참조하세요.

   액세스 키와 비밀 키는 각각 사용자 이름과 암호일 수 있습니다.

10. (선택 사항) 태그 추가를 선택하여 객체 스토리지 위치에 태그를 지정합니다.

    태그는 위치를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

11. 위치 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-location-object-storage`명령을 복사합니다.

```
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. 명령에서 다음 필수 파라미터를 지정합니다.

   - `--server-hostname` – 객체 스토리지 서버의 도메인 이름 또는 IP 주소를 지정합니다.
   - `--bucket-name` – 전송을 보내거나 받는 객체 스토리지 서버의 버킷 이름을 지정합니다.

3. (선택 사항) 명령에 다음 파라미터 중 하나를 추가합니다.

   - `--agent-arns` – 객체 스토리지 서버에 연결할 DataSync 에이전트를 지정합니다.
   - `--server-port` – 객체 스토리지 서버가 인바운드 네트워크 트래픽을 수락하는 포트(예: 포트 443)를 지정합니다.
   - `--server-protocol` – 객체 스토리지 서버의 통신에 사용되는 프로토콜(HTTP 또는 HTTPS)을 지정합니다.
   - `--access-key` – 객체 스토리지 서버에 인증하는 데 보안 인증이 필요한 경우 액세스 키(예: 사용자 이름)를 지정합니다.
   - `--secret-key` – 객체 스토리지 서버에 인증하는 데 보안 인증이 필요한 경우 보안 암호 키(예: 암호)를 지정합니다.

     또한 AWS Secrets Manager를 사용하여 키를 보호하기 위한 추가 파라미터를 제공할 수 있습니다. 자세한 내용은 스토리지 위치에 대한 자격 증명 제공을 참조하세요.
   - `--server-certificate`-시스템이 프라이빗 또는 자체 서명 인증 기관(CA)을 사용하는 경우 DataSync가 객체 스토리지 시스템으로 인증하기 위한 인증서 체인을 지정합니다. 전체 인증서 체인(예: `file:///home/user/.ssh/object_storage_certificates.pem`)이 있는 단일 `.pem` 파일을 지정해야 합니다.

     인증서 체인에는 다음이 포함될 수 있습니다.

     - 객체 스토리지 시스템의 인증서
     - 모든 중간 인증서(있는 경우)
     - 서명 CA의 루트 인증서

인증서를 .pem 파일로 연결할 수 있습니다(base64 인코딩 전 최대 32,768바이트). 다음 예제의 cat 명령은 세 개의 인증서가 포함된 *object_storage_certificates*.pem 파일을 생성합니다.

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

- --subdirectory – 객체 스토리지 서버의 객체 접두사를 지정합니다.

  DataSync는 이 접두사가 있는 객체만 복사합니다.

- --tags – 리소스에 추가하려는 태그를 나타내는 키-값 페어를 지정합니다.

  태그는 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 이름 태그를 생성하는 것이 좋습니다.

4. create-location-object-storage 명령을 실행합니다.

   방금 생성한 위치 ARN을 보여주는 응답을 받게 됩니다.

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

를 사용하여 AWS 스토리지로 또는 스토리지에서 전송 AWS DataSync

를 사용하면 여러 AWS 스토리지 서비스와 데이터를 주고받을 AWS DataSync수 있습니다. 자세한 내용은 Where can I transfer my data with DataSync? 섹션을 참조하세요.

주제

- Amazon S3를 사용하여 AWS DataSync 전송 구성
- Amazon EFS를 사용하여 AWS DataSync 전송 구성
- FSx for Windows File Server를 사용하여 전송 구성
- FSx for Lustre를 사용하여 DataSync 전송 구성
- Amazon FSx for OpenZFS를 사용하여 DataSync 전송 구성

- Amazon FSx for NetApp ONTAP를 사용하여 전송 구성

Amazon S3를 사용하여 AWS DataSync 전송 구성

Amazon S3 버킷에서 데이터를 전송하려면 AWS DataSync 전송 위치를 생성합니다. DataSync는 이 위치를 데이터 전송의 소스 또는 목적지로 사용할 수 있습니다.

DataSync에 S3 버킷 액세스 권한 제공

DataSync는 전송 중인 S3 버킷에 대한 액세스가 필요합니다. 이렇게 하려면 DataSync가 버킷에 액세스하는 데 필요한 권한으로 수임하는 AWS Identity and Access Management (IAM) 역할을 생성해야 합니다. DataSync의 Amazon S3 위치를 생성할 때 이 역할을 지정합니다.

목차

- 필수 권한
- DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성
- 서버측 암호화를 사용하여 S3 버킷에 액세스
- 제한된 S3 버킷 액세스
- VPC 액세스가 제한된 S3 버킷 액세스

필수 권한

IAM 역할에 필요한 권한은 버킷이 DataSync 소스인지 대상 위치인지에 따라 달라질 수 있습니다. Amazon S3 on Outposts에는 다른 권한 집합이 필요합니다.

Amazon S3 (source location)

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

```
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts"
              ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Amazon S3 (destination location)

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

```
            "s3:PutObjectTagging"
          ],
        "Effect": "Allow",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "123456789012"
            }
        }
    }
 ]
}
```

Amazon S3 on Outposts

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

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

DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성

콘솔에서 Amazon S3 위치를 생성할 때 DataSync는 일반적으로 S3 버킷에 액세스할 수 있는 적절한 권한을 가진 IAM 역할을 자동으로 생성하고 그 역할을 맡을 수 있습니다.

경우에 따라이 역할을 수동으로 생성해야 할 수 있습니다(예: 추가 보안 계층이 있는 버킷에 액세스하거나 다른의 버킷으로 또는 버킷에서 전송 AWS 계정).

DataSync를 위한 IAM 역할 수동 생성

1. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
2. 왼쪽 탐색 창의 액세스 관리에서 역할을 선택한 다음, 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택 페이지에서 신뢰할 수 있는 엔터티 유형으로 AWS 서비스를 선택합니다.
4. 사용 사례로 드롭다운 목록에서 DataSync를 선택하고 DataSync를 선택합니다. 다음을 선택합니다.
5. 권한 추가 페이지에서 다음을 선택합니다. 역할 이름을 제공하고 역할 생성을 선택합니다.
6. 역할 페이지에서 방금 생성한 역할의 이름을 검색해 선택합니다.
7. 역할의 세부 정보 페이지에서 권한 탭을 선택합니다. 권한 추가를 선택한 후 인라인 정책 추가를 선택합니다.
8. JSON 탭을 선택하고 버킷에 액세스하는 데 필요한 권한을 정책 편집기에 추가합니다.

9. 다음을 선택합니다. 정책에 이름을 제공하고 정책 생성을 선택합니다.
10. (권장) 교차 서비스 혼동된 대리자 문제를 방지하려면 다음을 수행합니다.

    a. 역할의 세부 정보 페이지에서 신뢰 관계 탭을 선택합니다. 신뢰 정책 편집을 선택합니다.

    b. `aws:SourceArn` 및 `aws:SourceAccount`전역 조건 컨텍스트 키가 포함된 다음 예를 사용하여 신뢰 정책을 업데이트하세요.

    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. 정책 업데이트를 선택합니다.

Amazon S3 위치를 생성할 때 이 역할을 지정할 수 있습니다.

서버측 암호화를 사용하여 S3 버킷에 액세스

DataSync는 서버측 암호화를 사용하는 S3 버킷으로 또는 S3 버킷에서 데이터를 전송할 수 있습니다. 버킷이 사용하는 암호화 키의 유형에 따라 DataSync가 버킷에 액세스할 수 있도록 허용하는 사용자 지정 정책이 필요한지 여부를 결정할 수 있습니다.

서버측 암호화를 사용하는 S3 버킷으로 DataSync를 사용할 때는 다음 사항을 기억하세요.

- S3 버킷이 AWS 관리형 키로 암호화된 경우 - 모든 리소스가 동일한 AWS 계정에 있는 경우 DataSync는 기본적으로 버킷의 객체에 액세스할 수 있습니다.
- S3 버킷이 고객 관리 AWS Key Management Service 형(AWS KMS) 키(SSE-KMS)로 암호화된 경우 - 키의 정책에 DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할이 포함되어야 합니다.
- S3 버킷이 고객 관리형 SSE-KMS 키 및 다른 로 암호화된 경우 AWS 계정 - DataSync는 다른의 버킷에 액세스할 수 있는 권한이 필요합니다 AWS 계정. 다음을 수행하여 이를 설정할 수 있습니다.
  - DataSync가 사용하는 IAM 역할에서 키의 정규화된 Amazon 리소스 이름(ARN)을 사용하여 교차 계정 버킷의 SSE-KMS 키를 지정해야 합니다. 버킷의 기본 암호화를 구성하는 데 사용하는 것과 동일한 키 ARN입니다. 이 상황에서는 키 ID, 별칭 이름 또는 별칭 ARN을 지정할 수 없습니다.

    다음은 키 ARN의 예제입니다.

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

    IAM 정책 문에서 KMS 키를 지정하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드를 참조하세요.
  - SSE-KMS 키 정책에서 DataSync에서 사용하는 IAM 역할을 지정합니다.
- 이중 계층 서버 측 암호화를 위해 S3 버킷을 고객 관리형 AWS KMS 키(DSSE-KMS)로 암호화하는 경우 - 키의 정책에 DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할이 포함되어야 합니다. (DSSE-KMS는 AWS KMS 요청 비용을 줄일 수 있는 S3 버킷 키를 지원하지 않습니다.)
- S3 버킷이 고객 제공 암호화 키(SSE-C)로 암호화된 경우 – DataSync가 이 버킷에 액세스할 수 없습니다.

예: DataSync에 대한 SSE-KMS 키 정책

다음 예제는 고객 관리형 SSE-KMS 키의 키 정책입니다. 정책은 서버측 암호화를 사용하는 S3 버킷에 연결됩니다.

다음 예제를 사용하려면 다음 값을 본인의 것으로 바꿉니다.

- *account-id* – AWS 계정.
- *admin-role-name* - 키를 관리할 수 있는 IAM 역할의 이름입니다.
- *datasync-role-name* - DataSync가 버킷에 액세스할 때 키를 사용하도록 허용하는 IAM 역할의 이름입니다.

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": "*"
        }
    ]
}
```

제한된 S3 버킷 액세스

일반적으로 모든 액세스를 거부하는 S3 버킷으로 또는 S3 버킷에서 전송해야 하는 경우, DataSync가 전송을 위해서만 버킷에 액세스할 수 있도록 버킷 정책을 편집할 수 있습니다.

예제: IAM 역할을 기반으로 액세스 허용

1. 다음 S3 버킷 정책을 복사합니다.

   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. 이 정책에서 다음 값을 바꿉니다.

   - *amzn-s3-demo-bucket* - 제한된 S3 버킷의 이름을 지정합니다.
   - *datasync-iam-role-id* - DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할의 ID를 지정합니다.

     다음 AWS CLI 명령을 실행하여 IAM 역할 ID를 가져옵니다.

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

     출력에서 `RoleId`값을 찾습니다.

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

   - *your-iam-role-id* - 버킷의 DataSync 위치를 생성하는 데 사용하는 IAM 역할의 ID를 지정합니다.

     다음 명령을 실행하여 IAM 역할 ID를 가져옵니다:

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

     출력에서 `RoleId`값을 찾습니다.

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

3. S3 버킷 정책에 이 정책을 추가합니다.
4. 제한된 버킷과 함께 DataSync 사용을 완료했으면 버킷 정책에서 두 IAM 역할의 조건을 모두 제거합니다.

VPC 액세스가 제한된 S3 버킷 액세스

특정 가상 프라이빗 클라우드(VPC) 엔드포인트 또는 VPC에 대한 액세스를 제한하는 Amazon S3 버킷은 DataSync가 해당 버킷으로 또는 버킷에서 전송하지 못하도록 거부합니다. 이러한 상황에서 전송을 활성화하려면 DataSync 위치에 지정한 IAM 역할을 포함하도록 버킷의 정책을 업데이트할 수 있습니다.

Option 1: Allowing access based on DataSync location role ARN

S3 버킷 정책에서 DataSync 위치 IAM 역할의 Amazon 리소스 이름(ARN)을 지정할 수 있습니다.

다음 예제는 두 VPC(`vpc-1234567890abcdef0` 및 `vpc-abcdef01234567890`)를 제외한 모든 VPC의 액세스를 거부하는 S3 버킷 정책입니다. 그러나 정책에는 DataSync 위치 역할의 ARN이 버킷에 액세스할 수 있는 ArnNotLikeIfExists 조건 및 aws:PrincipalArn 조건 키도 포함됩니다.

```
{
    "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

S3 버킷 정책에서 DataSync 위치 IAM 역할에 연결된 태그를 지정할 수 있습니다.

다음 예제는 두 VPC(`vpc-1234567890abcdef0` 및 `vpc-abcdef01234567890`)를 제외한 모든 VPC의 액세스를 거부하는 S3 버킷 정책입니다. 그러나 정책에는 태그 키 `exclude-from-`

`vpc-restriction`와 값이 `true`인 보안 주체를 허용하는 StringNotEqualsIfExists 조건 및 aws:PrincipalTag 조건 키도 포함됩니다. DataSync 위치 역할에 연결된 태그를 지정하여 버킷 정책에서 유사한 접근 방식을 시도할 수 있습니다.

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

Amazon S3 전송 시 스토리지 클래스 고려 사항

Amazon S3가 대상 위치인 경우, DataSync는 데이터를 특정 Amazon S3 스토리지 클래스로 직접 전송할 수 있습니다.

일부 스토리지 클래스에는 Amazon S3 스토리지 비용에 영향을 미칠 수 있는 동작이 있습니다. 객체 덮어쓰기, 삭제 또는 검색에 대한 추가 요금이 발생할 수 있는 스토리지 클래스를 사용하는 경우 객체 데이터나 메타데이터를 변경하면 해당 요금이 발생합니다. 자세한 내용은 Amazon S3 요금을 참조하세요.

> **Important**
>
> Amazon S3에 전송된 새 객체는 위치를 생성할 때 지정하는 스토리지 클래스를 사용하여 저장됩니다.

기본적으로 DataSync는 모든 데이터를 전송하도록 작업을 구성하지 않는 한 대상 위치에 있는 기존 객체의 스토리지 클래스를 보존합니다. 이러한 상황에서는 위치 생성 시 지정하는 스토리지 클래스가 모든 객체에 적용됩니다.

Amazon S3 스토리지 클래스	고려 사항
S3 Standard	S3 Standard을 선택하면 지리적으로 분리된 여러 가용 영역에 자주 액세스하는 파일을 중복 저장합니다. 이는 스토리지 클래스를 지정하지 않는 경우 기본값입니다.
S3 Intelligent-Tiering	S3 Intelligent-Tiering을 선택하면 가장 비용 효과적인 스토리지 액세스 계층으로 데이터를 자동으로 이동하여 스토리지 비용을 최적화합니다. S3 Intelligent-Tiering 스토리지 클래스에 저장된 객체에 대해 매월 요금을 지불합니다. 이 Amazon S3 요금에는 데이터 액세스 패턴 모니터링 및 티어 간 객체 이동이 포함됩니다.
S3 Standard-IA	S3 Standard_IA를 선택하면 지리적으로 분리된 여러 가용 영역에 자주 액세스하지 않는 객체를 중복 저장합니다. S3 Standard-IA 스토리지 클래스에 저장된 객체는 덮어쓰기, 삭제 또는 검색에 추가 비용을 발생시킬 수 있습니다. 이 객체가 얼마나 자주 변경되는지, 이 객체를 얼마나 오래 유지할 계획인지, 이 객체에 얼마나 자주 액세스해야 하는지 고려합니다. 객체 데이터 또는 메타데이터 변경은 객체를 삭제하고 이를 대체할 새 객체를 생성하는 것과 같습니다. 이로 인해 S3 Standard-IA 스토리지 클래스에 저장된 객체에 추가 요금이 발생합니다. 128KB 미만의 객체는 S3 Standard-IA 스토리지 클래스에서 객체당 최소 용량 요금보다 작습니다. 이러한 객체는 S3 Standard 스토리지 클래스에 저장됩니다.
S3 One Zone-IA	S3 One Zone-IA를 선택하면 단일 가용 영역에 자주 액세스하지 않는 객체를 저장합니다.

Amazon S3 스토리지 클래스	고려 사항
	S3 One Zone-IA 스토리지 클래스에 저장된 객체는 덮어쓰기, 삭제 또는 검색에 추가 비용을 발생시킬 수 있습니다. 이 객체가 얼마나 자주 변경되는지, 이 객체를 얼마나 오래 유지할 계획인지, 이 객체에 얼마나 자주 액세스해야 하는지 고려합니다. 객체 데이터 또는 메타데이터 변경은 객체를 삭제하고 이를 대체할 새 객체를 생성하는 것과 같습니다. 이로 인해 S3 One Zone-IA 스토리지 클래스에 저장된 객체에 추가 요금이 발생합니다. 128KB 미만의 객체는 S3 One Zone-IA 스토리지 클래스에서 객체당 최소 용량 요금보다 작습니다. 이러한 객체는 S3 Standard 스토리지 클래스에 저장됩니다.
S3 Glacier Instant Retrieval	거의 액세스하지 않지만 밀리초 단위로 검색해야 하는 객체를 아카이브하려면 S3 Glacier Instant Retrieval을 선택합니다. S3 Glacier Instant Retrieval 스토리지 클래스에 저장된 데이터는 동일한 대기 시간 및 처리량 성능의 S3 Standard-IA 스토리지 클래스보다 비용을 절감합니다. 그러나 S3 Glacier Instant Retrieval은 S3 Standard-IA보다 데이터 액세스 비용이 더 높습니다. S3 Glacier Instant Retrieval에 저장된 객체는 덮어쓰기, 삭제 또는 검색에 추가 비용을 발생시킬 수 있습니다. 이 객체가 얼마나 자주 변경되는지, 이 객체를 얼마나 오래 유지할 계획인지, 이 객체에 얼마나 자주 액세스해야 하는지 고려합니다. 객체 데이터 또는 메타데이터 변경은 객체를 삭제하고 이를 대체할 새 객체를 생성하는 것과 같습니다. 이로 인해 S3 Glacier Instant Retrieval 스토리지 클래스에 저장된 객체에 추가 요금이 발생합니다. 128KB 미만의 객체는 S3 Glacier Instant Retrieval 스토리지 클래스에서 객체당 최소 용량 요금보다 작습니다. 이러한 객체는 S3 Standard 스토리지 클래스에 저장됩니다.

Amazon S3 스토리지 클래스	고려 사항
S3 Glacier Flexible Retrieval	더 많은 활성 아카이브를 원하면 S3 Glacier Flexible Retrieval을 선택합니다. S3 Glacier Flexible Retrieval에 저장된 객체는 덮어쓰기, 삭제 또는 검색에 추가 비용을 발생시킬 수 있습니다. 이 객체가 얼마나 자주 변경되는지, 이 객체를 얼마나 오래 유지할 계획인지, 이 객체에 얼마나 자주 액세스해야 하는지 고려합니다. 객체 데이터 또는 메타데이터 변경은 객체를 삭제하고 이를 대체할 새 객체를 생성하는 것과 같습니다. 이로 인해 S3 Glacier Flexible Retrieval 스토리지 클래스에 저장된 객체에 추가 요금이 발생합니다. S3 Glacier Flexible Retrieval 스토리지 클래스에는 아카이빙된 각 객체에 대해 40KB의 추가 메타데이터가 필요합니다. DataSync는 40KB보다 작은 객체를 S3 Standard 스토리지 클래스에 저장합니다. DataSync에서 읽을 수 있으려면 먼저 이 스토리지 클래스에 보관된 객체를 복원해야 합니다. 해당 내용은 Amazon S3 사용 설명서의 아카이브된 객체 작업을 참조하세요. S3 Glacier Flexible Retrieval을 사용하는 경우 전송된 데이터만 확인을 선택하여 전송이 끝날 때 데이터와 메타데이터 체크섬을 비교합니다. 이 스토리지 클래스에는 대상의 모든 데이터 확인을 사용할 수 없습니다. 대상에서 기존의 모든 객체를 검색해야 하기 때문입니다.

Amazon S3 스토리지 클래스	고려 사항
S3 Glacier Deep Archive	객체를 장기 보관하고 데이터를 일년에 한 번이나 두 번 액세스하도록 디지털 보존하려면 S3 Glacier Deep Archive를 선택하세요. S3 Glacier Deep Archive에 저장된 객체는 덮어쓰기, 삭제 또는 검색에 추가 비용을 발생시킬 수 있습니다. 이 객체가 얼마나 자주 변경되는지, 이 객체를 얼마나 오래 유지할 계획인지, 이 객체에 얼마나 자주 액세스해야 하는지 고려합니다. 객체 데이터 또는 메타데이터 변경은 객체를 삭제하고 이를 대체할 새 객체를 생성하는 것과 같습니다. 이로 인해 S3 Glacier Deep Archive 스토리지 클래스에 저장된 객체에 추가 요금이 발생합니다. S3 Glacier Deep Archive 스토리지 클래스에는 아카이빙된 각 객체에 대해 40KB의 추가 메타데이터가 필요합니다. DataSync는 40KB보다 작은 객체를 S3 Standard 스토리지 클래스에 저장합니다. DataSync에서 읽을 수 있으려면 먼저 이 스토리지 클래스에 보관된 객체를 복원해야 합니다. 해당 내용은 Amazon S3 사용 설명서의 아카이브된 객체 작업을 참조하세요. S3 Glacier Deep Archive를 사용하는 경우 전송된 데이터만 확인을 선택하여 전송이 끝날 때 데이터와 메타데이터 체크섬을 비교합니다. 이 스토리지 클래스에는 대상의 모든 데이터 확인을 사용할 수 없습니다. 대상에서 기존의 모든 객체를 검색해야 하기 때문입니다.
S3 Outposts	Amazon S3 on Outposts에 대한 스토리지 클래스.

DataSync 사용 시 S3 요청 비용 평가

Amazon S3 위치를 사용하면 DataSync에서 수행한 S3 API 요청과 관련된 비용이 발생합니다. 이 섹션은 DataSync에서 이러한 요청을 사용하는 방식과 이러한 요청이 Amazon S3 비용에 미치는 영향을 이해하는 데 도움이 될 수 있습니다.

주제

- DataSync에서 수행한 S3 요청
- 비용 고려 사항

DataSync에서 수행한 S3 요청

다음 표에는 데이터를 Amazon S3 위치에 복사하거나 Amazon S3 위치에서 복사할 때 DataSync가 전송할 수 있는 S3 요청이 설명되어 있습니다.

S3 요청	DataSync에서 사용하는 방법
ListObjectV2	DataSync는 순방향 슬래시(/)로 끝나는 모든 객체에 대해 해당 접두사로 시작하는 객체를 나열하도록 하나 이상의 LIST요청을 수행합니다. 이 요청은 작업 준비 단계에서 호출됩니다.
HeadObject	DataSync는 작업의 준비 및 검증 단계에서 객체 메타데이터를 검색하도록 HEAD요청을 수행합니다. DataSync에서 전송하는 데이터의 무결성을 확인하는 방법에 따라 객체당 여러 HEAD요청이 있을 수 있습니다.
GetObject	DataSync는 작업 전송 단계에서 객체에서 데이터를 읽도록 GET요청을 수행합니다. 대용량 객체에 대해 여러 GET요청이 있을 수 있습니다.
GetObjectTagging	객체 태그를 복사하도록 작업을 구성하면 DataSync는 이러한 GET 요청에 따라 작업 준비 및 전송 단계에서 객체 태그 확인을 수행합니다.
PutObject	DataSync는 작업 전송 단계 중에 대상 S3 버킷에 객체와 접두사를 생성하도록 PUT요청을 수행합니다. DataSync는 Amazon S3 멀티파트 업로드 기능을 사용하므로 대용량 객체의 경우 여러 PUT요청이 있을 수 있습니다. 스토리지 비용을 최소화하려면 수명 주기 구성을 사용하여 미완료 멀티파트 업로드를 중지하는 것이 좋습니다.
PutObjectTagging	소스 객체에 태그가 있고 객체 태그를 복사하도록 작업을 구성한 경우, DataSync는 해당 태그를 전송할 때 이러한 PUT요청을 보냅니다.

S3 요청	DataSync에서 사용하는 방법
CopyObject	DataSync는 객체의 메타데이터가 변경된 경우에만 객체의 복사본을 생성하도록 COPY요청을 수행합니다. 이는 원래 메타데이터를 전달하지 않는 다른 서비스나 도구를 사용하여 S3 버킷에 데이터를 복사한 경우 발생할 수 있습니다.

비용 고려 사항

DataSync는 작업을 실행할 때마다 S3 버킷에서 S3 요청을 보냅니다. 이로 인해 특정 상황에서 요금이 누적될 수 있습니다. 예제:

- S3 버킷으로 또는 S3 버킷에서 객체를 전송하는 경우가 많습니다.
- 많은 데이터를 전송하지 않을 수도 있지만 S3 버킷에 많은 객체가 있습니다. DataSync가 각 버킷의 객체에 대해 S3 요청을 하기 때문에 이 시나리오에서도 여전히 높은 요금이 발생할 수 있습니다.
- S3 버킷 간에 전송을 수행하므로 DataSync는 소스와 대상에서 S3 요청을 보냅니다.

DataSync와 관련된 S3 요청 비용을 최소화하려면 다음 사항을 고려하세요.

주제

- 어떤 S3 스토리지 클래스를 사용하고 있습니까?
- 데이터를 얼마나 자주 전송해야 하나요?

어떤 S3 스토리지 클래스를 사용하고 있습니까?

S3 요청 요금은 특히 객체를 아카이브하는 클래스(S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval 및 S3 Glacier Deep Archive 클래스)의 경우 객체가 사용하는 Amazon S3 스토리지 클래스에 따라 달라질 수 있습니다.

다음은 DataSync를 사용할 때 스토리지 클래스가 S3 요청 요금에 영향을 미칠 수 있는 몇 가지 시나리오입니다.

- 작업을 실행할 때마다 DataSync가 객체 메타데이터를 검색하도록 HEAD요청을 수행합니다. 이러한 요청으로 인해 객체를 이동하지 않더라도 요금이 발생합니다. 이러한 요청이 청구서에 미치는 영향은 객체가 사용하는 스토리지 클래스와 DataSync가 스캔하는 객체 수에 따라 달라집니다.

- 객체를 S3 Glacier Instant Retrieval 스토리지 클래스로 이동하는 경우(직접 또는 버킷 수명 주기 구성을 통해), 이 클래스의 객체에 대한 요청은 다른 스토리지 클래스의 객체보다 비용이 많이 듭니다.
- 소스 및 대상 위치가 완전히 동기화되었는지 확인하도록 DataSync 작업을 구성하면 모든 스토리지 클래스(S3 Glacier Flexible Retrieval 및 S3 Glacier Deep Archive 제외)에서 각 객체에 대한 GET요청이 발생합니다.
- GET 요청에 더해 S3 Standard-IA, S3 One Zone-IA 또는 S3 Glacier Instant Retrieval 스토리지 클래스의 객체에 대한 데이터 검색 비용이 발생합니다.

자세한 내용은 Amazon S3 요금을 참조하세요.

데이터를 얼마나 자주 전송해야 하나요?

데이터를 반복적으로 이동해야 하는 경우 필요 이상으로 많은 작업을 실행하지 않는 일정을 고려하세요.

전송 범위를 제한하는 것도 고려할 수 있습니다. 예를 들어 특정 접두사의 객체에 초점을 맞추거나 전송되는 데이터를 필터링하도록 DataSync를 구성할 수 있습니다. 이러한 옵션은 DataSync 작업을 실행할 때마다 발생하는 S3 요청 수를 줄이는 데 도움이 될 수 있습니다.

Amazon S3 전송 시 객체 고려 사항

- S3 버킷에서 전송하는 경우 S3 Storage Lens를 사용하여 이동하는 객체 수를 파악합니다.
- S3 버킷 간에 전송할 때는 DataSync 작업 할당량이 적용되지 않으므로 확장 작업 모드를 사용하는 것이 좋습니다.
- 이름에 비표준 문자가 있는 경우 DataSync는 객체를 전송하지 않을 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 객체 키 명명 지침을 참조하세요.
- 버전 관리를 사용하는 S3 버킷으로 DataSync를 사용할 때는 다음 사항을 기억하세요.
  - S3 버킷으로 전송할 때 DataSync는 객체가 소스에서 수정된 경우 객체의 새 버전을 생성합니다. 이로 인해 추가 요금이 발생합니다.
  - 객체의 소스 버킷과 대상 버킷에서 버전 ID가 다릅니다.
  - 각 객체의 최신 버전만 소스 버킷에서 전송됩니다. 이전 버전은 대상으로 복사되지 않습니다.
- 처음에 S3 버킷에서 파일 시스템(예: NFS 또는 Amazon FSx)으로 데이터를 전송한 후 동일한 DataSync 작업의 후속 실행에는 수정되었지만 처음 전송할 때와 크기가 같은 객체는 포함되지 않습니다.

Amazon S3 범용 버킷의 전송 위치 생성

전송을 위한 위치를 생성하려면 기존 S3 범용 버킷이 필요합니다. 해당 버킷이 없는 경우 Amazon S3 사용 설명서를 참조하세요.

> **Important**
>
> 위치를 생성하기 전에 다음 섹션을 읽어야 합니다.
>
> - Amazon S3 전송 시 스토리지 클래스 고려 사항
> - DataSync 사용 시 S3 요청 비용 평가

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 Amazon S3를 선택한 다음 범용 버킷을 선택합니다.
4. S3 URI에는 사용자의 위치에 사용할 버킷과 접두사를 입력하거나 선택합니다.

   > **Warning**
   >
   > DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`

5. 대상으로 사용할 S3 스토리지 클래스에서 Amazon S3가 전송 대상일 때 객체가 사용할 스토리지 클래스를 선택합니다.

   자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항 단원을 참조하십시오.
6. IAM 역할에 대해 다음 중 하나를 수행합니다.

   - DataSync가 S3 버킷에 액세스하는 데 필요한 권한을 가진 IAM 역할을 자동으로 생성하도록 자동생성을 선택합니다.

이전에 DataSync에서 이 S3 버킷에 대한 IAM 역할을 만든 경우, 해당 역할이 기본적으로 선택됩니다.

- 생성한 사용자 지정 IAM 역할을 선택합니다. 자세한 내용은 DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성 단원을 참조하십시오.

7. (선택 사항) 새 태그 추가를 선택하여 Amazon S3 위치에 태그를 지정합니다.

   태그는 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 이름 태그를 생성하는 것이 좋습니다.

8. 위치 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-location-s3`명령을 복사합니다.

```
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. `--s3-bucket-arn`에서 위치로 사용할 S3 버킷의 ARN을 지정합니다.
3. `--s3-storage-class`에서 Amazon S3가 전송 대상일 때 객체가 사용할 스토리지 클래스를 지정합니다.
4. `--s3-config`에서 DataSync가 버킷에 액세스하는 데 필요한 IAM 역할의 ARN을 지정합니다.

   자세한 내용은 DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성 단원을 참조하십시오.

5. `--subdirectory`에서 DataSync가 읽거나 쓰는 S3 버킷의 접두사를 지정합니다(버킷이 소스인지 대상 위치인지에 따라 다름).

> **Warning**
>
> DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
>
> - `/photos`

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

6. create-location-s3 명령을 실행합니다.

   명령이 성공하면 생성한 위치의 ARN을 보여주는 응답을 받게 됩니다. 예제:

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

이 위치를 DataSync 작업의 소스 또는 대상으로 사용할 수 있습니다.

S3 on Outposts 버킷의 전송 위치 생성

전송을 위한 위치를 생성하려면 기존 Amazon S3 on Outposts 버킷이 필요합니다. 해당 버킷이 없는 경우 Amazon S3 on Outposts 사용 설명서를 참조하세요.

DataSync 에이전트도 필요합니다. 자세한 내용은 에 기본 모드 에이전트 배포 AWS Outposts 단원을 참조하십시오.

대용량 데이터세트(예: 수십만 개 또는 수백만 개의 객체)가 포함된 S3 on Outposts 버킷 접두사에서 전송하는 경우 DataSync 작업이 시간 초과될 수 있습니다. 이를 방지하려면 전송해야 하는 정확한 객체를 지정할 수 있는 DataSync 매니페스트를 사용하는 것이 좋습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 Amazon S3를 선택한 다음 Outposts 버킷을 선택합니다.
4. S3 버킷에서 S3 on Outposts 버킷에 액세스할 수 있는 Amazon S3 액세스 포인트를 선택합니다.

   자세한 내용은 Amazon S3 사용 설명서를 참조하세요.
5. 대상으로 사용할 S3 스토리지 클래스에서 Amazon S3가 전송 대상일 때 객체가 사용할 스토리지 클래스를 선택합니다.

자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항 단원을 참조하십시오. DataSync는 기본적으로 Amazon S3 on Outposts용 S3 Outposts 스토리지 클래스를 사용합니다.

6. 에이전트에서 Outpost의 DataSync 에이전트에 대한 Amazon 리소스 이름(ARN)을 지정합니다.
7. 폴더에 DataSync가 읽거나 쓰는 S3 버킷의 접두사를 입력합니다(버킷이 소스인지 대상 위치인지에 따라 다름).

> **Warning**
>
> DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`
> - `photos/../2006/March`

8. IAM 역할에 대해 다음 중 하나를 수행합니다.
   - DataSync가 S3 버킷에 액세스하는 데 필요한 권한을 가진 IAM 역할을 자동으로 생성하도록 자동생성을 선택합니다.

     이전에 DataSync에서 이 S3 버킷에 대한 IAM 역할을 만든 경우, 해당 역할이 기본적으로 선택됩니다.
   - 생성한 사용자 지정 IAM 역할을 선택합니다. 자세한 내용은 DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성 단원을 참조하십시오.
9. (선택 사항) 새 태그 추가를 선택하여 Amazon S3 위치에 태그를 지정합니다.

   태그는 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 이름 태그를 생성하는 것이 좋습니다.
10. 위치 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-location-s3`명령을 복사합니다.

```
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. `--s3-bucket-arn`에서 S3 on Outposts 버킷에 액세스할 수 있는 Amazon S3 액세스 포인트의 ARN을 선택합니다.

   자세한 내용은 Amazon S3 사용 설명서를 참조하세요.

3. `--s3-storage-class`에서 Amazon S3가 전송 대상일 때 객체가 사용할 스토리지 클래스를 지정합니다.

   자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항 단원을 참조하십시오. DataSync는 기본적으로 S3 on Outposts용 S3 Outposts 스토리지 클래스를 사용합니다.

4. `--s3-config`에서 DataSync가 버킷에 액세스하는 데 필요한 IAM 역할의 ARN을 지정합니다.

   자세한 내용은 DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성 단원을 참조하십시오.

5. `--subdirectory`에서 DataSync가 읽거나 쓰는 S3 버킷의 접두사를 지정합니다(버킷이 소스인지 대상 위치인지에 따라 다름).

   > **Warning**
   >
   > DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`

6. `--agent-arns`에서 Outpost에 있는 DataSync 에이전트의 ARN을 지정합니다.
7. `create-location-s3` 명령을 실행합니다.

   명령이 성공하면 생성한 위치의 ARN을 보여주는 응답을 받게 됩니다. 예제:

```
{
```

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

이 위치를 DataSync 작업의 소스 또는 대상으로 사용할 수 있습니다.

를 통한 Amazon S3 전송 AWS 계정

DataSync를 사용하면 다른 AWS 계정에서 데이터를 S3 버킷으로 또는 S3 버킷에서 이동할 수 있습니다. 자세한 내용은 다음 튜토리얼을 참조하세요.

- 를 통해 온프레미스 스토리지에서 Amazon S3로 데이터 전송 AWS 계정
- 에서 Amazon S3에서 Amazon S3로 데이터 전송 AWS 계정

상용 및 간의 Amazon S3 전송 AWS GovCloud (US) Regions

기본적으로 DataSync는 상용 및 AWS GovCloud (US) Regions의 S3 버킷 간에 전송하지 않습니다. 하지만 전송 시 S3 버킷 중 하나에 대한 객체 스토리지 위치를 생성하여 이러한 전송 유형을 설정할 수 있습니다. 에이전트를 사용하거나 사용하지 않고 이러한 유형의 전송을 수행할 수 있습니다. 에이전트를 사용하는 경우 작업을 기본 모드로 구성해야 합니다. 에이전트 없이 전송하려면 확장 모드를 사용해야 합니다.

시작하기 전에: 리전 간 전송으로 인한 비용 영향을 이해해야 합니다 자세한 내용은 AWS DataSync 요금을 참조하세요.

목차

- DataSync에 객체 스토리지 위치의 버킷 액세스 권한 제공
- DataSync 에이전트 생성(선택 사항)
- S3 버킷의 객체 스토리지 위치 생성

DataSync에 객체 스토리지 위치의 버킷 액세스 권한 제공

이 전송을 위한 객체 스토리지 위치를 생성할 때 DataSync에 해당 위치의 S3 버킷에 액세스할 수 있는 권한과 함께 IAM 사용자의 자격 증명을 제공해야 합니다. 자세한 내용은 필수 권한 단원을 참조하십시오.

> **Warning**
>
> IAM 사용자는 장기 자격 증명을 가지므로 보안 위험이 있습니다. 이 위험을 줄이려면 이러한 사용자에게 작업을 수행하는 데 필요한 권한만 제공하고 더 이상 필요하지 않을 경우 이러한 사용자를 제거하는 것이 좋습니다.

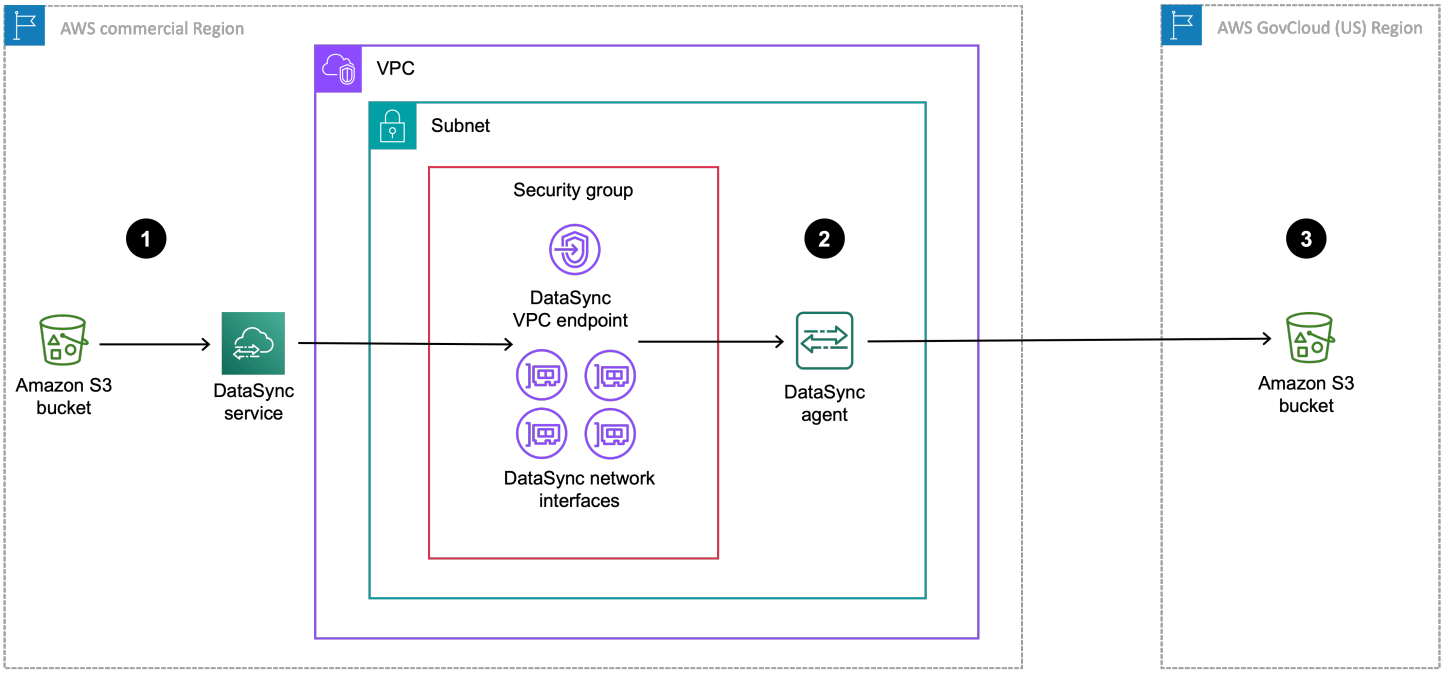
DataSync 에이전트 생성(선택 사항)

기본 모드를 사용하여 전송을 실행하려면 에이전트를 사용해야 합니다. 상용 및 간에 전송하기 때문에 DataSync 에이전트를 리전 중 하나에 Amazon EC2 인스턴스로 AWS GovCloud (US) Region배포합니다. 퍼블릭 인터넷으로의 데이터 전송 요금을 방지하려면 에이전트가 VPC 서비스 엔드포인트를 사용하는 것이 좋습니다. 자세한 내용은 Amazon EC2 Data 데이터 전송 요금을 참조하세요.

DataSync 작업을 실행하려는 리전을 기반으로 에이전트를 생성하는 방법을 설명하는 다음 시나리오 중 하나를 선택합니다.

상용 리전에서 DataSync 작업을 실행하는 경우

다음 다이어그램은 DataSync 작업과 에이전트가 상용 리전에 있는 전송을 보여줍니다.



레퍼런스	설명
1	DataSync 작업을 실행하는 상용 리전에서 소스 S3 버킷으로부터 데이터를 전송합니다. 소스 버킷은 상용 리전의 Amazon S3 위치로 구성됩니다.
2	VPC 서비스 엔드포인트 및 네트워크 인터페이스가 있는 동일한 VPC 및 서브넷에 있는 DataSync 에이전트를 통해 데이터를 전송합니다.
3	AWS GovCloud (US) Region의 대상 S3 버킷으로 데이터를 전송합니다. 대상 버킷은 상용 리전의 객체 스토리지 위치로 구성됩니다.

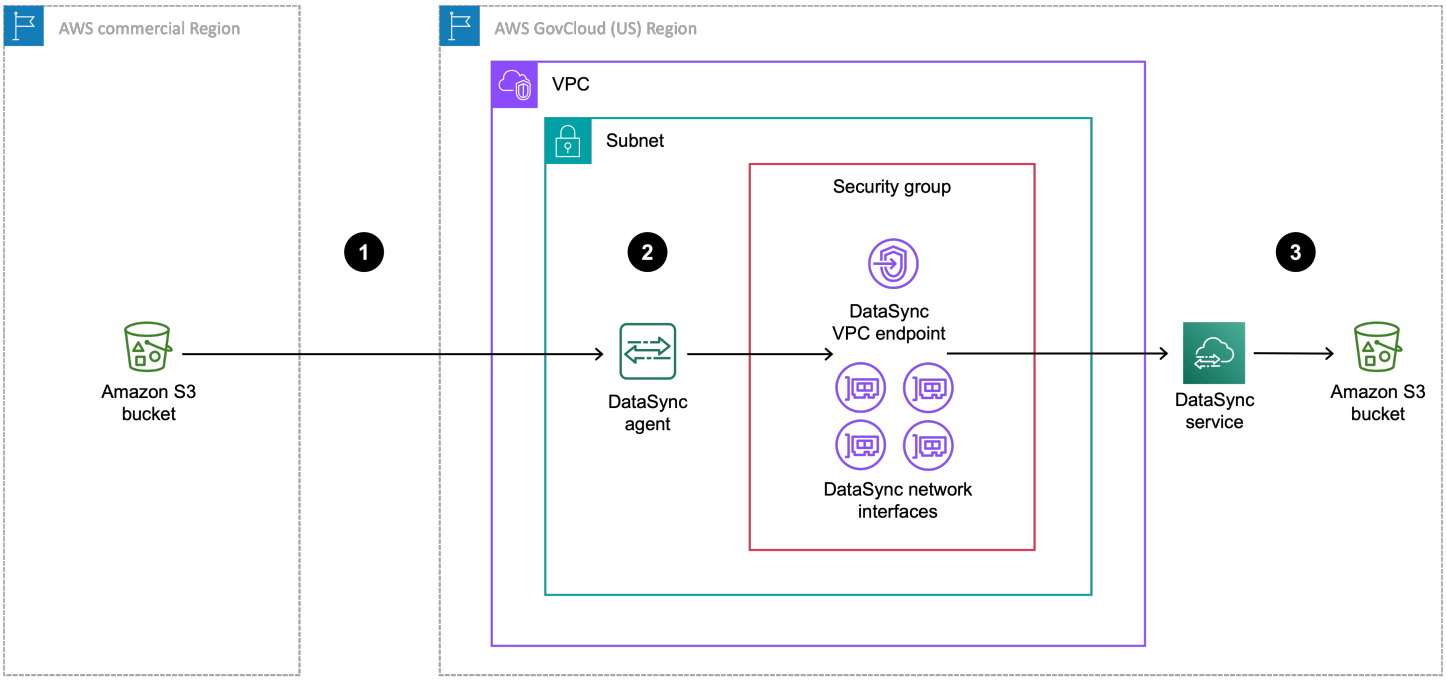
이 동일한 설정을 사용하여 반대 방향을에서 상용 리전 AWS GovCloud (US) Region 으로 전송할 수도 있습니다.

DataSync 에이전트를 생성하려면

1. 상용 리전에 Amazon EC2 에이전트를 배포합니다.
2. VPC 서비스 엔드포인트를 사용하도록 에이전트를 구성합니다.
3. 에이전트 활성화.

GovCloud(미국) 리전에서 DataSync 작업을 실행하는 경우

다음 다이어그램은 DataSync 작업과 에이전트가 AWS GovCloud (US) Region에 있는 전송을 보여줍니다.



레퍼런스	설명
1	상용 리전의 소스 S3 버킷에서 DataSync 작업을 실행하는 AWS GovCloud (US) Region 로 데이터를 전송합니다. 소스 버킷은 AWS GovCloud (US) Region에서 객체 스토리지 위치로 구성됩니다.
2	에서 AWS GovCloud (US) Region데이터는 VPC 서비스 엔드포인트 및 네트워크 인터페이스가 위치한 동일한 VPC 및 서브넷의 DataSync 에이전트를 통해 전송됩니다.
3	AWS GovCloud (US) Region의 대상 S3 버킷으로 데이터를 전송합니다. 대상 버킷은 AWS GovCloud (US) Region에서 Amazon S3 위치로 구성됩니다.

이 동일한 설정을 사용하여 반대 방향을에서 상용 리전 AWS GovCloud (US) Region 으로 전송할 수도 있습니다.

DataSync 에이전트를 생성하려면

1. 에 Amazon EC2 에이전트를 배포합니다 AWS GovCloud (US) Region.
2. VPC 서비스 엔드포인트를 사용하도록 에이전트를 구성합니다.

3. 에이전트 활성화.

데이터세트의 압축성이 높으면 AWS GovCloud (US) Region에서 작업을 실행하는 동안 상용 리전에서 에이전트를 생성하여 비용을 절감할 수 있습니다. 상용 리전에서 사용할 에이전트 준비를 포함하여 이 에이전트를 생성하는 데 평소보다 설정이 더 많습니다. 이 설정을 위한 에이전트 생성에 대한 자세한 내용은를 사용하여 안팎 AWS GovCloud (US) 으로 데이터 이동 블로그를 참조하세요 AWS DataSync.

S3 버킷의 객체 스토리지 위치 생성

DataSync 작업을 실행하지 않는 리전에 있는 S3 버킷의 객체 스토리지 위치가 필요합니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 작업을 실행하려는 리전과 동일한 리전에 있어야 합니다.
3. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
4. 위치 유형에서 객체 스토리지를 선택합니다.
5. 에이전트에서 이 전송을 위해 생성한 DataSync 에이전트를 선택합니다.
6. 서버에서 다음 형식 중 하나를 사용하여 버킷의 Amazon S3 엔드포인트를 입력합니다.

   - 상용 리전 버킷: `s3.your-region.amazonaws.com`
   - AWS GovCloud (US) Region 버킷: `s3.your-gov-region.amazonaws.com`

   Amazon S3 엔드포인트 목록은 AWS 일반 참조 섹션을 참조하세요.
7. 버킷 이름에서 S3 버킷의 이름을 입력합니다.
8. 폴더에 DataSync가 읽거나 쓰는 S3 버킷의 접두사를 입력합니다(버킷이 소스인지 대상 위치인지에 따라 다름).

> **Warning**
>
> DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`

- photos/../2006/March

9. 자격 증명 필요를 선택하고 다음을 수행합니다.
   - 액세스 키에서 버킷에 액세스할 수 있는 IAM 사용자의 액세스 키를 입력합니다.
   - 보안 키에서 동일한 IAM 사용자의 보안 키를 입력합니다.
10. (선택 사항) 태그 추가를 선택하여 위치에 태그를 지정합니다.

    태그는 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 이름 태그를 생성하는 것이 좋습니다.
11. 위치 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-location-object-storage`명령을 복사합니다.

```
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. `--server-hostname` 파라미터에 다음 형식 중 하나를 사용하여 버킷에 대한 Amazon S3 엔드포인트를 지정합니다.
   - 상용 리전 버킷: `s3.your-region.amazonaws.com`
   - AWS GovCloud (US) Region 버킷: `s3.your-gov-region.amazonaws.com`

   엔드포인트의 리전에서 작업을 실행하려는 리전과 동일한 리전을 지정해야 합니다.

   Amazon S3 엔드포인트 목록은 AWS 일반 참조 섹션을 참조하세요.
3. `--bucket-name` 파라미터에서 S3 버킷의 이름을 지정합니다.
4. `--agent-arns` 파라미터에서 이 전송을 위해 생성한 DataSync 에이전트를 지정합니다.
5. `--access-key` 파라미터에서 버킷에 액세스할 수 있는 IAM 사용자의 액세스 키를 지정합니다.
6. `--secret-key` 파라미터에서 동일한 IAM 사용자의 보안 키를 입력합니다.
7. (선택 사항) `--subdirectory` 파라미터에서 DataSync가 읽거나 쓰는 S3 버킷의 접두사를 입력합니다(버킷이 소스인지 대상 위치인지에 따라 다름).

> **Warning**
>
> DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`
> - `photos/../2006/March`

8. (선택 사항) `--tags` 파라미터에서 위치 리소스의 태그를 나타내는 키-값 페어를 지정합니다.

   태그는 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 이름 태그를 생성하는 것이 좋습니다.

9. `create-location-object-storage` 명령을 실행합니다.

   방금 생성한 위치 ARN을 보여주는 응답을 받게 됩니다.

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

이 위치를 DataSync 작업의 소스 또는 대상으로 사용할 수 있습니다. 이 전송의 다른 S3 버킷에서 Amazon S3 위치를 생성합니다.

다음 단계

몇 가지 가능한 다음 단계는 다음과 같습니다.

1. 필요한 경우 다른 위치를 생성합니다. 자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
2. 전송할 파일, 메타데이터 처리 방법 등 DataSync 작업 설정을 구성합니다.
3. DataSync 작업 일정을 설정합니다.
4. DataSync 작업에 대한 모니터링을 구성합니다.
5. 작업을 시작합니다.

Amazon EFS를 사용하여 AWS DataSync 전송 구성

Amazon EFS 파일 시스템으로 또는 Amazon EFS 파일 시스템에서 데이터를 전송하려면 AWS DataSync 전송 위치를 생성해야 합니다. DataSync는 이 위치를 데이터 전송의 소스 또는 목적지로 사용할 수 있습니다.

DataSync에 Amazon EFS 파일 시스템 액세스 권한 제공

위치를 생성하려면 DataSync가 스토리지에 액세스하는 방법을 이해해야 합니다. Amazon EFS에서 DataSync는 네트워크 인터페이스를 사용하여 가상 프라이빗 클라우드(VPC)에서 루트 사용자로 파일 시스템을 탑재합니다.

목차

- 탑재 대상의 서브넷 및 보안 그룹 확인
- 제한된 파일 시스템 액세스
  - 파일 시스템 액세스를 위한 DataSync IAM 역할 생성
  - DataSync 액세스를 허용하는 파일 시스템 정책 예제

탑재 대상의 서브넷 및 보안 그룹 확인

위치를 생성할 때 DataSync가 Amazon EFS 파일 시스템의 탑재 대상 중 하나에 연결하도록 허용하는 서브넷 및 보안 그룹을 지정합니다.

지정한 서브넷은 다음과 같이 위치해야 합니다.

- 파일 시스템과 동일한 VPC
- 하나 이상의 파일 시스템 탑재 대상과 동일한 가용 영역

> **Note**
>
> 파일 시스템 탑재 대상을 포함하는 서브넷을 지정할 필요가 없습니다.

지정하는 보안 그룹은 Network File System(NFS) 포트 2049에서 인바운드 트래픽을 허용해야 합니다. 탑재 대상의 보안 그룹 생성 및 업데이트에 대한 자세한 내용은 Amazon EFS 사용 설명서를 참조하세요.

탑재 대상과 연결된 보안 그룹 지정

파일 시스템의 탑재 대상 중 하나와 연결된 보안 그룹을 지정할 수 있습니다. 네트워크 관리 관점에서 이 접근 방식을 사용하는 것이 좋습니다.

탑재 대상과 연결되지 않은 보안 그룹 지정

파일 시스템의 탑재 대상 중 하나와 연결되지 않은 보안 그룹을 지정할 수도 있습니다. 그러나 이 보안 그룹은 탑재 대상의 보안 그룹과 통신할 수 있어야 합니다.

예를 들어 보안 그룹 D(DataSync용)와 보안 그룹 M(탑재 대상영) 간의 관계를 생성하는 방법은 다음과 같습니다.

- 위치를 생성할 때 지정하는 보안 그룹 D에는 NFS 포트 2049에서 보안 그룹 M으로의 아웃바운드 연결을 허용하는 규칙이 있어야 합니다.
- 탑재 대상과 연결되는 보안 그룹 M은 보안 그룹 D의 NFS 포트 2049에서 인바운드 액세스를 허용해야 합니다.

탑재 대상의 보안 그룹을 찾으려면

다음 지침은 DataSync가 전송에 사용할 Amazon EFS 파일 시스템 탑재 대상의 보안 그룹을 식별하는 데 도움이 될 수 있습니다.

1. 에서 다음 `describe-mount-targets` 명령을 AWS CLI실행합니다.

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

이 명령은 파일 시스템의 탑재 대상에 대한 정보를 반환합니다(다음 예제 출력과 유사).

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

```
        }
    ]
}
```

2. 사용하려는 `MountTargetId` 값을 기록해 둡니다.
3. `MountTargetId`를 사용하는 다음 `describe-mount-target-security-groups` 명령을 실행하면 탑재 대상의 보안 그룹을 찾을 수 있습니다.

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

위치를 생성할 때 이 보안 그룹을 지정합니다.

제한된 파일 시스템 액세스

DataSync는 액세스 포인트 및 IAM 정책을 통해 액세스를 제한하는 Amazon EFS 파일 시스템으로 또는 Amazon EFS 파일 시스템에서 전송할 수 있습니다.

> **Note**
>
> DataSync가 사용자 자격 증명을 적용하는 액세스 포인트를 통해 대상 파일 시스템에 액세스하는 경우, 소유권을 복사하도록 DataSync 작업을 구성하면 소스 데이터의 POSIX 사용자 및 그룹 ID가 보존되지 않습니다. 대신 전송된 파일 및 폴더는 액세스 포인트의 사용자 및 그룹 ID로 설정됩니다. 이 경우 DataSync가 소스 및 대상 위치의 메타데이터 간 불일치를 감지하기 때문에 작업 확인이 실패합니다.

목차

- 파일 시스템 액세스를 위한 DataSync IAM 역할 생성
- DataSync 액세스를 허용하는 파일 시스템 정책 예제

파일 시스템 액세스를 위한 DataSync IAM 역할 생성

IAM 정책을 통해 액세스를 제한하는 Amazon EFS 파일 시스템이 있는 경우 DataSync에 파일 시스템에서 데이터를 읽거나 쓸 수 있는 권한을 제공하는 IAM 역할을 생성할 수 있습니다. 그런 다음 파일 시스템 정책에서 해당 역할을 지정해야 할 수 있습니다.

DataSync IAM 역할을 생성하려면

1. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
2. 왼쪽 탐색 창의 액세스 관리에서 역할을 선택한 다음, 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택 페이지에서 신뢰할 수 있는 엔터티 유형으로 사용자 지정 신뢰 정책을 선택합니다.
4. 다음 JSON을 정책 편집기에 붙여넣습니다.

   JSON

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

5. 다음을 선택합니다. 권한 추가 페이지에서 다음을 선택합니다.
6. 역할 이름을 제공하고 역할 생성을 선택합니다.

위치를 생성할 때 이 역할을 지정합니다.

DataSync 액세스를 허용하는 파일 시스템 정책 예제

다음 예제 파일 시스템 정책은 Amazon EFS 파일 시스템(정책에서 `fs-1234567890abcdef0`로 식별됨)에 대한 액세스가 제한되지만 *MyDataSyncRole*이라는 IAM 역할을 통해 DataSync에 대한 액세스를 허용하는 방법을 보여줍니다.

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` - DataSync에 파일 시스템에 대한 액세스 권한을 부여하는 IAM 역할을 지정합니다.
- `Action` - DataSync에 루트 액세스 권한을 부여하고 파일 시스템에서 읽고 쓸 수 있게 합니다.
- `aws:SecureTransport` - 파일 시스템에 연결할 때 NFS 클라이언트가 TLS를 사용하도록 요구합니다.
- `elasticfilesystem:AccessPointArn` - 특정 액세스 포인트를 통해서만 파일 시스템에 액세스할 수 있습니다.

Amazon EFS 전송 시 네트워크 고려 사항

DataSync와 함께 사용하는 VPC에는 기본 테넌시가 있어야 합니다. 전용 테넌시가 있는 VPC는 지원되지 않습니다.

Amazon EFS 전송 시 성능 고려 사항

Amazon EFS 파일 시스템의 처리량 모드는 전송 기간 및 전송 중 파일 시스템 성능에 영향을 미칠 수 있습니다. 다음을 고려하세요.

- 최상의 결과를 얻으려면 탄력적 처리량 모드를 사용하는 것이 좋습니다. 탄력적 처리량 모드를 사용하지 않는 경우 전송 시간이 더 오래 걸릴 수 있습니다.
- 버스트 처리량 모드를 사용하는 경우 DataSync가 파일 시스템 버스트 크레딧을 사용하기 때문에 파일 시스템 애플리케이션의 성능이 영향을 받을 수 있습니다.
- 전송된 데이터를 확인하도록 DataSync를 구성하는 방법은 파일 시스템 성능 및 데이터 액세스 비용에 영향을 미칠 수 있습니다.

자세한 내용은 Amazon Elastic File System 사용 설명서의 Amazon EFS performance 및 Amazon EFS 요금 페이지를 참조하세요.

Amazon EFS 전송 위치 생성

전송 위치를 생성하려면 기존 Amazon EFS 파일 시스템이 필요합니다. 파일 시스템이 없는 경우 Amazon Elastic File System 사용 설명서의 Amazon EFS 시작하기를 참조하세요.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형으로 Amazon EFS 파일 시스템을 선택합니다.

   나중에 이 위치를 소스 또는 대상 주소로서 구성합니다.
4. 파일 시스템에서 위치로 사용하려는 Amazon EFS 파일 시스템을 선택합니다.
5. 마운트 경로에는 Amazon EFS 파일 시스템의 마운트 경로를 입력합니다.

   DataSync가 파일 시스템의 데이터를 읽거나 쓰는 위치를 지정합니다(소스 위치인지 대상 위치인지에 따라 다름).

   기본적으로 DataSync는 루트 디렉터리(또는 EFS 액세스 포인트 설정에 루트 디렉터리를 제공하는 경우 액세스 포인트)를 사용합니다. 전방향 슬래시(예: `/path/to/directory`)를 사용하여 하위 디렉터리를 지정할 수도 있습니다.
6. 서브넷에서 DataSync가 데이터 전송 트래픽 관리를 위한 네트워크 인터페이스를 생성하는 서브넷을 선택합니다.

   서브넷은 다음 위치에 있어야 합니다.

   - 파일 시스템과 동일한 VPC
   - 하나 이상의 파일 시스템 탑재 대상과 동일한 가용 영역.

> **Note**
>
> 파일 시스템 탑재 대상을 포함하는 서브넷을 지정할 필요가 없습니다.

7. 보안 그룹에서 Amazon EFS 파일 시스템의 탑재 대상과 연결된 보안 그룹을 선택합니다. 보안 그룹을 두 개 이상 선택할 수 있습니다.

   > **Note**
   >
   > 지정하는 보안 그룹은 NFS 포트 2049에서 인바운드 트래픽을 허용해야 합니다. 자세한 내용은 탑재 대상의 서브넷 및 보안 그룹 확인 단원을 참조하십시오.

8. 전송 중 암호화에서 DataSync가 파일 시스템으로 또는 파일 시스템에서 데이터를 전송할 때 Transport Layer Security(TLS) 암호화를 사용할지 여부를 선택합니다.

   > **Note**
   >
   > Amazon EFS 위치에 따라 액세스 포인트, IAM 역할 또는 둘 다를 구성하려면 이 설정을 활성화해야 합니다.

9. (선택 사항) EFS 액세스 포인트에서 DataSync가 파일 시스템을 탑재하는 데 사용할 수 있는 액세스 포인트를 선택합니다.

   자세한 내용은 제한된 파일 시스템 액세스 단원을 참조하십시오.

10. (선택 사항) IAM 역할에는 DataSync가 파일 시스템에 액세스할 수 있도록 허용하는 역할을 지정합니다.

    이 역할을 생성하는 방법에 대한 자세한 내용은 파일 시스템 액세스를 위한 DataSync IAM 역할 생성 섹션을 참조하세요.

11. (선택 사항) 태그 추가를 선택하여 파일 시스템에 태그를 지정합니다.

    태그는 위치를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다.

12. 위치 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-location-efs`명령을 복사합니다.

```
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. `--efs-filesystem-arn`에서, 전송할 Amazon EFS 파일 시스템의 Amazon 리소스 이름(ARN)을 지정합니다.
3. `--subdirectory`에서 파일 시스템의 탑재 경로를 지정합니다.

   DataSync가 파일 시스템의 데이터를 읽거나 쓰는 위치입니다(소스 위치인지 대상 위치인지에 따라 다름).

   기본적으로 DataSync는 루트 디렉터리(또는 사용자가 `--access-point-arn`에 루트 디렉터리를 제공하는 경우 액세스 포인트)를 사용합니다. 전방향 슬래시(예: `/path/to/directory`)를 사용하여 하위 디렉터리를 지정할 수도 있습니다.
4. `--ec2-config`에서 다음을 수행합니다.

   - `SecurityGroupArns`에서 파일 시스템의 탑재 대상과 연결된 보안 그룹의 ARN을 지정합니다. 보안 그룹을 두 개 이상 지정할 수 있습니다.

     > **Note**
     >
     > 지정하는 보안 그룹은 NFS 포트 2049에서 인바운드 트래픽을 허용해야 합니다. 자세한 내용은 탑재 대상의 서브넷 및 보안 그룹 확인 단원을 참조하십시오.

   - `SubnetArn`에서 DataSync가 데이터 전송 트래픽 관리를 위한 네트워크 인터페이스를 생성하는 서브넷의 ARN을 지정합니다.

     서브넷은 다음 위치에 있어야 합니다.

     - 파일 시스템과 동일한 VPC
     - 하나 이상의 파일 시스템 탑재 대상과 동일한 가용 영역.

> **Note**
>
> 파일 시스템 탑재 대상을 포함하는 서브넷을 지정할 필요가 없습니다.

5. `--in-transit-encryption`에서 DataSync가 파일 시스템으로 또는 파일 시스템에서 데이터를 전송할 때 Transport Layer Security(TLS) 암호화를 사용할지 여부를 지정합니다.

> **Note**
>
> Amazon EFS 위치에 따라 액세스 포인트, IAM 역할 또는 둘 다를 구성하려면 이것을 `TLS1_2`로 설정해야 합니다.

6. (선택 사항) `--access-point-arn`에서 DataSync가 파일 시스템을 탑재하는 데 사용할 수 있는 액세스 포인트의 ARN을 지정합니다.

   자세한 내용은 제한된 파일 시스템 액세스 단원을 참조하십시오.

7. (선택 사항) `--file-system-access-role-arn`에서 DataSync가 파일 시스템에 액세스하도록 허용하는 IAM 역할의 ARN을 지정합니다.

   이 역할을 생성하는 방법에 대한 자세한 내용은 파일 시스템 액세스를 위한 DataSync IAM 역할 생성 섹션을 참조하세요.

8. `create-location-efs` 명령을 실행합니다.

   명령이 성공하면 생성한 위치의 ARN을 보여주는 응답을 받게 됩니다. 예제:

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

FSx for Windows File Server를 사용하여 전송 구성

Amazon FSx for Windows File Server 파일 시스템과의 데이터 전송을 수행하려면 AWS DataSync 전송 위치를 생성해야 합니다. DataSync는 이 위치를 데이터 전송의 소스 또는 목적지로 사용할 수 있습니다.

DataSync에 FSx for Windows File Server 파일 시스템 액세스 권한 제공

DataSync는 Server Message Block(SMB) 프로토콜을 사용하여 FSx for Windows File Server 파일 시스템에 연결하고 네트워크 인터페이스를 사용하여 가상 프라이빗 클라우드(VPC)에서 파일 시스템을 탑재합니다.

> **Note**
>
> DataSync와 함께 사용하는 VPC에는 기본 테넌시가 있어야 합니다. 전용 테넌시가 있는 VPC는 지원되지 않습니다.

주제

- 필수 권한
- 필요한 인증 프로토콜
- DFS 네임스페이스

필수 권한

DataSync에 FSx for Windows File Server 파일, 폴더 및 파일 메타데이터를 탑재하고 액세스하는 데 필요한 권한을 제공해야 합니다.

이 사용자는 파일 시스템을 관리하기 위해 Microsoft Active Directory 그룹에 속하는 것이 좋습니다. 이 그룹의 세부 정보는 Active Directory 설정에 따라 달라집니다.

- FSx for Windows File Server와 AWS Directory Service for Microsoft Active Directory 함께를 사용하는 경우 사용자는 AWS 위임된 FSx 관리자 그룹의 멤버여야 합니다.
- FSx for Windows File Server에 자체 관리형 Active Directory를 사용하는 경우 사용자는 두 그룹 중 하나의 멤버여야 합니다.
  - 기본 위임된 관리자 그룹인 도메인 관리자 그룹입니다.
  - DataSync가 객체 소유권 권한 및 Windows 액세스 제어 목록(ACL)을 복사하도록 허용하는 사용자 권한이 있는 사용자 지정 위임형 관리자 그룹입니다.

> **Important**
>
> 파일 시스템이 배포된 후에는 위임된 관리자 그룹을 변경할 수 없습니다. DataSync가 메타데이터를 복사하는 데 필요한 다음 사용자 권한과 함께 사용자 지정 위임된 관리자 그룹을 사용하려면 파일 시스템을 재배포하거나 백업에서 복원해야 합니다.

사용자 권한	설명
파일 및 디렉터리 복원(SE_RESTORE_NAME)	DataSync가 객체 소유권, 권한, 파일 메타데이터, NTFS 임의 액세스 목록(DACL)을 복사하도록 허용합니다. 이 사용자 권한은 일반적으로 도메인 관리자 및 백업 운영자 그룹(둘 다 기본 Active Directory 그룹)의 멤버에게 부여됩니다.
감사 및 보안 로그 관리(SE_SECURITY_NAME)	DataSync가 NTFS 시스템 액세스 제어 목록(SACL)을 복사하도록 허용합니다. 이 사용자 권한은 일반적으로 도메인 관리자 그룹의 멤버에게 부여됩니다.

- Windows ACL을 복사하고, SMB 파일 서버와 FSx for Windows File Server 파일 시스템 간에 또는 FSx for Windows File Server 파일 시스템 간에 전송하려면 DataSync를 제공하는 사용자는 동일한 Active Directory 도메인에 속하거나 도메인 간에 Active Directory 신뢰 관계가 있어야 합니다.

> **Warning**
>
> FSx for Windows File Server 파일 시스템의 SYSTEM 사용자는 파일 시스템의 모든 폴더에 대한 전체 제어 권한이 있어야 합니다. 폴더에서 이 사용자의 NTFS ACL 권한을 변경하지 마세요. 이 경우 DataSync는 파일 공유에 액세스할 수 없게 하고 파일 시스템 백업을 사용할 수 없게 하는 방식으로 파일 시스템의 권한을 변경할 수 있습니다. 파일 및 폴더 수준 액세스에 대한 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서를 참조하세요.

필요한 인증 프로토콜

DataSync에서 액세스하려면 FSx for Windows File Server가 NTLM 인증을 사용해야 합니다. DataSync는 Kerberos 인증을 사용하는 파일 서버에 액세스할 수 없습니다.

DFS 네임스페이스

DataSync는 Microsoft 분산 파일 시스템(DFS) 네임스페이스를 지원하지 않습니다. DataSync 위치를 생성할 때 기본 파일 서버 또는 공유를 지정하는 것이 좋습니다.

자세한 내용은 Amazon FSx for Windows File Server 사용 설명서의 Grouping multiple file systems with DFS Namespaces 섹션을 참조하세요.

FSx for Windows File Server 전송 위치 생성

시작하기 전에 AWS 리전에 기존 FSx for Windows File Server가 있는지 확인합니다. 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서의 Amazon FSx 시작하기를 참조하세요.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 Amazon FSx를 선택합니다.
4. FSx 파일 시스템에는 위치로 사용하려는 FSx for Windows File Server 파일 시스템을 선택합니다.
5. 공유 이름에는 순방향 슬래시를 사용하여 FSx for Windows File Server의 마운트 경로를 입력합니다.

   이렇게 하면 DataSync가 데이터를 읽거나 쓰는 경로를 지정합니다(소스 위치인지 대상 위치인지에 따라 다름).

   하위 디렉터리도 포함할 수 있습니다(예: `/path/to/directory`).
6. 보안 그룹에는 파일 시스템의 기본 설정 서브넷에 대한 액세스를 제공하는 Amazon EC2 보안 그룹을 최대 5개까지 선택합니다.

   선택한 보안 그룹은 파일 시스템의 보안 그룹과 통신할 수 있어야 합니다. 파일 시스템 액세스를 위한 보안 그룹 구성에 대한 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서를 참조하세요.

> **Note**
>
> 보안 그룹 자체 내 내부 연결을 허용하지 않는 보안 그룹을 선택한 경우 다음 중 하나를 수행합니다.
>
> - 보안 그룹 자체 내 통신을 허용하도록 보안 그룹 구성을 구성합니다.
> - 탑재 대상의 보안 그룹과 통신할 수 있는 다른 보안 그룹을 선택합니다.

7. 사용자에서 FSx for Windows File Server에 액세스할 수 있는 사용자 이름을 입력합니다.

   자세한 내용은 필수 권한 단원을 참조하십시오.

8. 암호에서 사용자 이름의 암호를 입력합니다.
9. (선택 사항) 도메인에서 FSx for Windows File Server 파일 시스템이 속한 Windows 도메인의 이름을 입력합니다.

   환경에 여러 Active Directory 도메인이 있는 경우 이 설정을 구성하면 DataSync가 올바른 파일 시스템에 연결되게 할 수 있습니다.

10. (선택 사항) 키와 값 필드에는 FSx for Windows File Server에 태그를 지정하기 위한 값을 입력합니다.

    태그는 AWS 리소스를 관리, 필터링 및 검색하는 데 도움이 됩니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

11. 위치 생성을 선택합니다.

사용 AWS CLI

를 사용하여 FSx for Windows File Server 위치를 생성하려면 AWS CLI

- 다음 명령을 사용하여 Amazon FSx 위치를 생성합니다.

```
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
```

`create-location-fsx-windows` 명령에서 다음을 수행합니다.

- `fsx-filesystem-arn`-전송으로 주고받을 파일 시스템의 Amazon 리소스 이름(ARN)을 지정합니다.
- `security-group-arns`-파일 시스템의 기본 설정 서브넷에 대한 액세스를 제공하는 Amazon EC2 보안 그룹 최대 5개의 ARN을 지정합니다.

  지정한 보안 그룹은 파일 시스템의 보안 그룹과 통신할 수 있어야 합니다. 파일 시스템 액세스를 위한 보안 그룹 구성에 대한 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서를 참조하세요.

  > **Note**
  >
  > 보안 그룹 자체 내 내부 연결을 허용하지 않는 보안 그룹을 선택한 경우 다음 중 하나를 수행합니다.
  >
  > - 보안 그룹 자체 내 통신을 허용하도록 보안 그룹 구성을 구성합니다.
  > - 탑재 대상의 보안 그룹과 통신할 수 있는 다른 보안 그룹을 선택합니다.

- AWS 리전 - 지정하는 리전은 대상 Amazon FSx 파일 시스템이 위치한 리전입니다.

위의 명령은 다음 중 한 가지와 유사한 위치 ARN을 반환합니다.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07db7abfc326c50fb"
}
```

FSx for Lustre를 사용하여 DataSync 전송 구성

Amazon FSx for Lustre 파일 시스템으로 또는 Amazon FSx for Lustre 파일 시스템에서 데이터를 전송하려면 AWS DataSync 전송 위치를 생성해야 합니다. DataSync는 이 위치를 데이터 전송의 소스 또는 목적지로 사용할 수 있습니다.

DataSync에 FSx for Lustre 파일 시스템 액세스 권한 제공

DataSync는 Lustre 클라이언트를 사용하여 FSx for Lustre 파일 시스템에 액세스합니다. DataSync를 사용하려면 FSx for Lustre 파일 시스템에 있는 모든 데이터에 대한 액세스 권한이 필요합니다. DataSync는 이 액세스 수준을 갖기 위해 `0`의 사용자 ID(UID)와 그룹 ID(GID)를 사용하여 루트 사용자로 파일 시스템을 마운트합니다.

DataSync는 네트워크 인터페이스를 사용하여 Virtual Private Cloud(VPC)에서 파일 시스템을 마운트합니다. DataSync는 사용자를 대신하여 이러한 네트워크 인터페이스의 생성, 사용 및 삭제를 완전히 관리합니다.

> **Note**
>
> DataSync와 함께 사용하는 VPC에는 기본 테넌시가 있어야 합니다. 전용 테넌시가 있는 VPC는 지원되지 않습니다.

FSx for Lustre 전송 위치 생성

전송 위치를 생성하려면 기존 FSx for Lustre 파일 시스템이 필요합니다. 자세한 내용은 Amazon FSx for Lustre 사용 설명서의 Amazon FSx for Lustre 시작하기를 참조하세요.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 Amazon FSx를 선택합니다.

   나중에 이 위치를 소스 또는 대상 주소로서 구성합니다.
4. FSx 파일 시스템에는 위치로 사용하려는 FSx for Lustre 파일 시스템을 선택합니다.
5. 마운트 경로에는 FSx for Lustre 파일 시스템의 마운트 경로를 입력합니다.

   경로에는 하위 디렉터리가 포함될 수 있습니다. 위치가 소스로 사용되는 경우 DataSync는 마운트 경로에서 데이터를 읽습니다. 위치가 대상으로 사용되는 경우 DataSync는 모든 데이터를 마운트 경로에 씁니다. 하위 디렉터리가 제공되지 않는 경우 DataSync는 루트 디렉터리(/)를 사용합니다.
6. 보안 그룹에서 FSx for Lustre 파일 시스템에 대한 액세스를 제공하는 보안 그룹을 최대 5개까지 선택합니다.

   보안 그룹은 파일 시스템의 포트에 액세스할 수 있어야 합니다. 또한 파일 시스템은 보안 그룹의 액세스를 허용해야 합니다.

   보안 그룹에 대한 자세한 내용은 Amazon FSx for Lustre 사용 설명서의 Amazon VPC로 파일 시스템 액세스 제어를 참조하세요.
7. (선택 사항) 키와 값 필드에는 FSx for Lustre 파일 시스템에 태그를 지정하기 위한 값을 입력합니다.

태그는 AWS 리소스를 관리, 필터링 및 검색하는 데 도움이 됩니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

8. 위치 생성을 선택합니다.

사용 AWS CLI

를 사용하여 FSx for Lustre 위치를 생성하려면 AWS CLI

- 다음 명령을 사용하여 FSx for Lustre 위치를 생성합니다.

```
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
```

다음 파라미터는 `create-location-fsx-lustre`명령의 필수 파라미터입니다.

- `fsx-filesystem-arn` – 읽거나 쓰려는 파일 시스템의 정규화된 Amazon 리소스 이름(ARN)입니다.
- `security-group-arns` – 파일 시스템의 기본 설정 서브넷의 네트워크 인터페이스에 적용하는 Amazon EC2 보안 그룹의 ARN입니다.

위의 명령은 다음과 유사한 위치 ARN을 반환합니다.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07sb7abfc326c50fb"
}
```

Amazon FSx for OpenZFS를 사용하여 DataSync 전송 구성

Amazon FSx for OpenZFS 파일 시스템으로 또는 Amazon FSx for OpenZFS 파일 시스템에서 데이터를 전송하려면 AWS DataSync 전송 위치를 생성해야 합니다. DataSync는 이 위치를 데이터 전송의 소스 또는 목적지로 사용할 수 있습니다.

DataSync에 FSx for OpenZFS 파일 시스템 액세스 권한 제공

DataSync는 네트워크 인터페이스를 사용하여 Virtual Private Cloud(VPC)에서 FSx for OpenZFS 파일 시스템을 마운트합니다. DataSync는 사용자를 대신하여 이러한 네트워크 인터페이스의 생성, 사용 및 삭제를 완전히 관리합니다.

> **Note**
>
> DataSync와 함께 사용하는 VPC에는 기본 테넌시가 있어야 합니다. 전용 테넌시가 있는 VPC는 지원되지 않습니다.

FSx for OpenZFS 파일 시스템 인증 구성

DataSync는 NFS 클라이언트로 FSx for OpenZFS 파일 시스템에 액세스하여 `0`의 사용자 ID(UID)와 그룹 ID(GID)를 사용해 루트 사용자로 파일 시스템을 마운트합니다.

DataSync가 모든 파일 메타데이터를 복사하려면(`no_root_squash`을)를 사용하여 파일 시스템 볼륨의 NFS 내보내기 설정을 구성해야 합니다. 하지만 이 액세스 수준을 특정 DataSync 작업으로만 제한할 수 있습니다.

자세한 내용을 알아보려면 Amazon FSx for OpenZFS User Guide(Amazon FSx for OpenZFS 사용 설명서)의 Volume properties(볼륨 속성)를 참조하세요.

DataSync 고유 NFS 내보내기 구성(권장)

DataSync 작업에서만 액세스하는 각 볼륨에만 해당하는 NFS 내보내기를 구성할 수 있습니다. 이 작업은 FSx for OpenZFS 위치를 생성할 때 지정한 마운트 경로의 가장 최근 상위 볼륨에 대해 수행합니다.

DataSync 고유 NFS 내보내기를 구성하려면

1. DataSync 작업을 생성합니다.

   이를 통해 NFS 내보내기 설정에서 지정할 작업의 네트워크 인터페이스를 생성합니다.
2. Amazon EC2 콘솔 또는를 사용하여 작업 네트워크 인터페이스의 프라이빗 IP 주소를 찾습니다 AWS CLI.
3. FSx for OpenZFS 파일 시스템 볼륨에는 다음과 같이 각 작업의 네트워크 인터페이스의 NFS 내보내기 설정을 구성합니다.

   - 클라이언트 주소: 네트워크 인터페이스의 프라이빗 IP 주소(예: *10.24.34.0*)를 입력합니다.

- NFS 옵션: `rw,no_root_squash`를 입력합니다.

모든 클라이언트에 대한 NFS 내보내기 구성

모든 클라이언트에 대한 루트 액세스를 허용하는 NFS 내보내기를 지정할 수 있습니다.

모든 클라이언트에 대해 NFS 내보내기를 구성하려면

- FSx for OpenZFS 파일 시스템 볼륨에는 다음과 같이 NFS 내보내기 설정을 구성합니다.
  - 클라이언트 주소: `*`를 입력합니다.
  - NFS 옵션: `rw,no_root_squash`를 입력합니다.

FSx for OpenZFS 전송 위치 생성

위치를 생성하려면 기존 FSx for OpenZFS 파일 시스템이 필요합니다. 파일 시스템이 없는 경우 Amazon FSx for OpenZFS 사용 설명서의 Amazon FSx for OpenZFS 시작하기를 참조하세요.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 위치를 선택한 다음 위치 생성을 선택합니다.
3. 위치 유형에서 Amazon FSx를 선택합니다.

   나중에 이 위치를 소스 또는 대상 주소로서 구성합니다.
4. FSx 파일 시스템에는 위치로 사용하려는 FSx for OpenZFS 파일 시스템을 선택합니다.
5. 마운트 경로에는 FSx for OpenZFS 파일 시스템의 마운트 경로를 입력합니다.

   경로는 `/fsx`로 시작해야 하며 파일 시스템의 기존 디렉토리 경로일 수 있습니다. 위치가 소스로 사용되는 경우 DataSync는 마운트 경로에서 데이터를 읽습니다. 위치가 대상으로 사용되는 경우 DataSync는 모든 데이터를 마운트 경로에 씁니다. 하위 디렉터리가 제공되지 않는 경우 DataSync는 루트 볼륨 디렉터리(예: `/fsx`)를 사용합니다.
6. 보안 그룹에서 FSx for OpenZFS 파일 시스템에 대한 네트워크 액세스를 제공하는 보안 그룹을 최대 5개까지 선택합니다.

   보안 그룹은 FSx for OpenZFS 파일 시스템이 사용하는 네트워크 포트에 대한 액세스를 제공해야 합니다. 파일 시스템은 보안 그룹의 네트워크 액세스를 허용해야 합니다.

보안 그룹에 대한 자세한 내용은 Amazon FSx for OpenZFS 사용 설명서의 Amazon VPC로 파일 시스템 액세스 제어를 참조하세요.

7. (선택 사항) 추가 설정을 확장하고 NFS 버전으로 DataSync가 파일 서버에 액세스할 때 사용하는 NFS 버전을 선택합니다.

   기본적으로 DataSync는 NFS 버전 4.1을 사용합니다.

8. (선택 사항) 키와 값 필드에는 FSx for OpenZFS 파일 시스템에 태그를 지정하기 위한 값을 입력합니다.

   태그는 위치에 대한 관리, 필터링 및 검색에 도움이 됩니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

9. 위치 생성을 선택합니다.

사용 AWS CLI

를 사용하여 FSx for OpenZFS 위치를 생성하려면 AWS CLI

1. 다음 `create-location-fsx-open-zfs`명령을 복사합니다.

```
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. 명령에서 다음 필수 옵션을 지정합니다.

   - `fsx-filesystem-arn`에 위치 파일 시스템의 정규화된 Amazon 리소스 이름(ARN)을 지정합니다. 여기에는 파일 시스템이 AWS 리전 있는 , AWS 계정및 파일 시스템 ID가 포함됩니다.
   - `security-group-arns`에 FSx for OpenZFS 파일 시스템의 기본 설정 서브넷의 네트워크 인터페이스에 대한 액세스를 제공하는 Amazon EC2 보안 그룹의 ARN을 지정합니다. 여기에는 Amazon EC2 인스턴스 AWS 리전 가 있는 , AWS 계정및 보안 그룹 ID가 포함됩니다.

     보안 그룹에 대한 자세한 내용은 Amazon FSx for OpenZFS 사용 설명서의 Amazon VPC로 파일 시스템 액세스 제어를 참조하세요.

   - `protocol`에서 DataSync가 파일 시스템에 액세스하는 데 사용하는 프로토콜을 지정합니다. (DataSync는 현재 NFS만 지원합니다.)

3. 명령을 실행합니다. 방금 생성한 위치를 보여주는 응답을 받게 됩니다.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890"
}
```

Amazon FSx for NetApp ONTAP를 사용하여 전송 구성

Amazon FSx for NetApp ONTAP 파일 시스템으로 또는 Amazon FSx for NetApp ONTAP 파일 시스템에서 데이터를 전송하려면 AWS DataSync 전송 위치를 생성해야 합니다. DataSync는 이 위치를 데이터 전송의 소스 또는 목적지로 사용할 수 있습니다.

DataSync에 FSx for ONTAP 파일 시스템 액세스 권한 제공

FSx for ONTAP 파일 시스템에 액세스하기 위해 DataSync는 Virtual Private Cloud(VPC)의 네트워크 인터페이스를 사용하여 파일 시스템에 스토리지 가상 머신(SVM)을 마운트합니다. DataSync는 FSx for ONTAP 위치를 포함하는 작업을 생성할 때만 파일 시스템의 기본 설정 서브넷에서 이러한 네트워크 인터페이스를 생성합니다.

> **Note**
>
> DataSync와 함께 사용하는 VPC에는 기본 테넌시가 있어야 합니다. 전용 테넌시가 있는 VPC는 지원되지 않습니다.

DataSync는 Network File System(NFS) 또는 Server Message Block(SMB) 프로토콜을 사용하여 FSx for ONTAP 파일 시스템의 SVM에 연결하고 데이터를 복사할 수 있습니다.

주제

- NFS 프로토콜 사용
- SMB 프로토콜 사용
- 지원되지 않는 프로토콜
- 올바른 프로토콜 선택
- SnapLock 볼륨 액세스

NFS 프로토콜 사용

NFS 프로토콜을 사용하는 경우 DataSync는 `0`의 사용자 ID(UID) 및 그룹 ID(GID)로 `AUTH_SYS` 보안 메커니즘을 사용하여 SVM을 인증합니다.

> **Note**
>
> DataSync는 현재 FSx for ONTAP 위치에 대해 NFS 버전 3만 지원합니다.

SMB 프로토콜 사용

SMB 프로토콜을 사용하는 경우 DataSync는 사용자가 제공한 자격 증명을 사용하여 SVM을 인증합니다.

지원되는 SMB 버전

기본적으로 DataSync는 SMB 파일 서버와의 협상을 기반으로 SMB 프로토콜 버전을 자동으로 선택합니다. 특정 버전을 사용하도록 DataSync를 구성할 수도 있지만 DataSync가 SMB 파일 서버와 자동으로 협상하는 데 문제가 있는 경우에만 이렇게 하는 것이 좋습니다. 보안상의 이유로 SMB 버전 3.0.2 이상을 사용하는 것이 좋습니다.

FSx for ONTAP 위치를 사용하여 SMB 버전을 구성하기 위한 DataSync 콘솔 및 API의 옵션 목록은 다음 표를 참조하세요.

콘솔 옵션	API 옵션	설명
자동	`AUTOMATIC`	DataSync와 SMB 파일 서버는 2.1과 3.1.1 사이에서 상호 지원하는 SMB의 가장 높은 버전을 협상합니다. 이는 기본값이며 권장 옵션입니다. 대신 파일 서버에서 지원하지 않는 특정 버전을 선택하면 `Operation Not Supported` 오류가 발생할 수 있습니다.
SMB 3.0.2	`SMB3`	프로토콜 협상을 SMB 버전 3.0.2로만 제한합니다.
SMB 2.1	`SMB2`	프로토콜 협상을 SMB 버전 2.1로만 제한합니다.
SMB 2.0	`SMB2_0`	프로토콜 협상을 SMB 버전 2.0으로만 제한합니다.

필수 권한

SVM의 로컬 사용자 또는 Microsoft Active Directory의 도메인 사용자가 파일, 폴더 및 파일 메타데이터를 탑재하고 액세스하는 데 필요한 권한을 DataSync에 제공해야 합니다.

Active Directory에서 사용자를 제공하는 경우, 다음 사항에 유의하세요.

- AWS Directory Service for Microsoft Active Directory를 사용하는 경우 사용자는 AWS 위임된 FSx 관리자 그룹의 멤버여야 합니다.
- 자체 관리형 Active Directory를 사용하는 경우 사용자는 두 그룹 중 하나의 멤버여야 합니다.
  - 기본 위임된 관리자 그룹인 도메인 관리자 그룹입니다.
  - DataSync가 객체 소유권 권한 및 Windows 액세스 제어 목록(ACL)을 복사하도록 허용하는 사용자 권한이 있는 사용자 지정 위임형 관리자 그룹입니다.

> **Important**
>
> 파일 시스템이 배포된 후에는 위임된 관리자 그룹을 변경할 수 없습니다. DataSync가 메타데이터를 복사하는 데 필요한 다음 사용자 권한과 함께 사용자 지정 위임된 관리자 그룹을 사용하려면 파일 시스템을 재배포하거나 백업에서 복원해야 합니다.

사용자 권한	설명
운영 체제의 일부로 작동(SE_TCB_NAME)	DataSync가 객체 소유권, 권한, 파일 메타데이터, NTFS 임의 액세스 목록(DACL)을 복사하도록 허용합니다. 이 사용자 권한은 일반적으로 도메인 관리자 및 백업 운영자 그룹(둘 다 기본 Active Directory 그룹)의 멤버에게 부여됩니다.
감사 및 보안 로그 관리(SE_SECURITY_NAME)	DataSync가 NTFS 시스템 액세스 제어 목록(SACL)을 복사하도록 허용합니다. 이 사용자 권한은 일반적으로 도메인 관리자 그룹의 멤버에게 부여됩니다.

- Windows ACL을 복사하고, SMB를 사용하는 FSx for ONTAP 파일 시스템(또는 SMB를 사용하는 다른 파일 시스템 유형) 간에 전송하려면 DataSync를 제공하는 사용자는 동일한 Active Directory 도메인에 속하거나 도메인 간에 Active Directory 신뢰 관계가 있어야 합니다.

필요한 인증 프로토콜

DataSync에서 SMB 공유에 액세스하려면 FSx for ONTAP 파일 시스템이 반드시 NTLM 인증을 사용해야 합니다. DataSync는 Kerberos 인증을 사용하는 FSx for ONTAP 파일 서버에 액세스할 수 없습니다.

DFS 네임스페이스

DataSync는 Microsoft 분산 파일 시스템(DFS) 네임스페이스를 지원하지 않습니다. DataSync 위치를 생성할 때 기본 파일 서버 또는 공유를 지정하는 것이 좋습니다.

지원되지 않는 프로토콜

DataSync는 iSCSI(Internet Small Computer Systems Interface) 프로토콜을 사용하여 FSx for ONTAP 파일 시스템에 액세스할 수 없습니다.

올바른 프로토콜 선택

FSx for ONTAP 마이그레이의에서 파일 메타데이터를 보존하려면 DataSync 소스 및 대상 위치가 동일한 프로토콜을 사용하도록 구성하세요. 지원되는 프로토콜 사이에서 SMB는 메타데이터를 가장 높은 충실도로 보존합니다(자세한 내용은 DataSync가 파일 및 객체 메타데이터를 처리하는 방법 이해참조).

NFS를 통해 사용자에게 서비스를 제공하는 Unix(Linux) 서버 또는 네트워크 연결 스토리지(NAS) 공유에서 마이그레이션할 때는 다음을 수행하세요.

1. Unix(Linux) 서버 또는 NAS 공유를 위한 NFS 위치를 생성합니다. (여기가 소스 위치가 됩니다.)
2. Unix 보안 스타일을 사용하여 데이터를 전송하는 FSx for ONTAP 볼륨을 구성합니다.
3. NFS용으로 구성된 FSx for ONTAP 파일 시스템에 위치를 생성합니다. (여기가 대상 위치가 됩니다.)

SMB를 통해 사용자에게 서비스를 제공하는 Windows 서버 또는 NAS 공유에서 마이그레이션할 때는 다음을 수행하세요.

1. Windows 서버 또는 NAS 공유를 위한 SMB 위치를 생성합니다. (여기가 소스 위치가 됩니다.)
2. NTFS 보안 스타일을 사용하여 데이터를 전송하는 FSx for ONTAP 볼륨을 구성합니다.

3. SMB용으로 구성된 FSx for ONTAP 파일 시스템에 위치를 생성합니다. (여기가 대상 위치가 됩니다.)

FSx for ONTAP 환경에서 여러 프로토콜을 사용하는 경우 AWS 스토리지 전문가와 협력하는 것이 좋습니다. 멀티프로토콜 액세스의 모범 사례에 대해 알아보려면 Amazon FSx for NetApp ONTAP를 사용하여 멀티프로토콜 워크로드 활성화를 참조하세요.

SnapLock 볼륨 액세스

FSx for ONTAP 파일 시스템의 SnapLock 볼륨으로 데이터를 전송하는 경우 전송 중 볼륨에서 SnapLock 설정 자동 커밋 및 볼륨 추가 모드가 비활성화되어 있는지 확인합니다. 데이터 전송이 완료되면 이러한 설정을 다시 활성화할 수 있습니다.

FSx for ONTAP 전송 위치 생성

위치를 생성하려면 기존 FSx for ONTAP 파일 시스템이 필요합니다. 파일 시스템이 없는 경우 Amazon FSx for NetApp ONTAP 사용 설명서의 Amazon FSx for NetApp ONTAP 시작하기를 참조하세요.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 Amazon FSx를 선택합니다.

   나중에 이 위치를 소스 또는 대상 주소로서 구성합니다.
4. FSx 파일 시스템에는 위치로 사용하려는 FSx for ONTAP 파일 시스템을 선택합니다.
5. 스토리지 가상 머신에서는 데이터를 복사하려는 파일 시스템의 스토리지 가상 머신(SVM)을 선택합니다.
6. 마운트 경로에는 데이터를 복사할 SVM의 파일 공유 경로를 지정합니다.

   정션 경로(탑재 지점이라고도 함), qtree 경로(NFS 파일 공유의 경우) 또는 공유 이름(SMB 파일 공유의 경우)을 지정할 수 있습니다. 예를 들어, 탑재 경로는 `/vol1`, `/vol1/tree1`또는 `/share1`일 수 있습니다.

   > **Tip**
   >
   > SVM의 루트 볼륨에 경로를 지정하지 않습니다. 자세한 설명은 Amazon FSx for NetApp ONTAP User Guide(Amazon FSx for NetApp ONTAP 사용자 가이드)의 Managing FSx

for ONTAP storage virtual machines(FSx for ONTAP 스토리지 가상 머신 관리)를 참조하세요.

7. 보안 그룹에는 파일 시스템의 기본 설정 서브넷에 대한 액세스를 제공하는 Amazon EC2 보안 그룹을 최대 5개까지 선택합니다.

   보안 그룹은 다음 포트에서 아웃바운드 트래픽을 허용해야 합니다(사용 중인 프로토콜에 따라 다름).

   - NFS - TCP 포트 111, 635 및 2049
   - SMB - TCP 포트 445

   파일 시스템의 보안 그룹은 동일한 포트에서 인바운드 트래픽도 허용해야 합니다.

8. 프로토콜에는 DataSync가 파일 시스템의 SVM에 액세스하는 데 사용하는 데이터 전송 프로토콜을 선택합니다.

   자세한 설명은 올바른 프로토콜 선택섹션을 참조하세요.

   NFS

   DataSync는 NFS 버전 3을 사용합니다.

   SMB

   SVM에 액세스하려면 SMB 버전, 사용자, 암호, Active Directory 도메인 이름(필요한 경우)을 구성합니다.

   - (선택 사항) 추가 설정을 확장하고 DataSync가 SVM에 액세스할 때 사용할 SMB 버전을 선택합니다.

     기본적으로 DataSync는 SMB 파일 서버와의 협상을 기반으로 버전을 자동으로 선택합니다. 자세한 내용은 SMB 프로토콜 사용 단원을 참조하십시오.
   - 사용자에서 SVM에서 전송할 파일, 폴더, 메타데이터를 탑재하고 이에 액세스할 수 있는 사용자 이름을 입력합니다.

     자세한 내용은 SMB 프로토콜 사용 단원을 참조하십시오.
   - 암호에서 SVM에 액세스할 수 있다고 지정한 사용자의 암호를 입력합니다.
   - (선택 사항) Active Directory 도메인 이름에 SVM이 속한 Active Directory의 정규화된 도메인 이름(FQDN)을 입력합니다.

환경에 여러 도메인이 있는 경우 이 설정을 구성하면 DataSync가 올바른 SVM에 연결되게 할 수 있습니다.

9. (선택 사항) 키와 값 필드에는 FSx for ONTAP 파일 시스템에 태그를 지정하기 위한 값을 입력합니다.

   태그는 AWS 리소스를 관리, 필터링 및 검색하는 데 도움이 됩니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

10. 위치 생성을 선택합니다.

사용 AWS CLI

를 사용하여 FSx for ONTAP 위치를 생성하려면 AWS CLI

1. 다음 `create-location-fsx-ontap`명령을 복사합니다.

```
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. 명령에서 다음 필수 옵션을 지정합니다.

   - `storage-virtual-machine-arn`에 데이터를 복사하려는 파일 시스템에서 스토리지 가상 머신(SVM)의 정규화된 Amazon 리소스 이름(ARN)을 지정합니다.

     이 ARN에는 파일 시스템이 AWS 리전 있는 , AWS 계정및 파일 시스템 및 SVM IDs 포함됩니다.

   - `security-group-arns`에 파일 시스템의 기본 설정 서브넷의 네트워크 인터페이스에 대한 액세스를 제공하는 Amazon EC2 보안 그룹의 ARN을 지정합니다.

     여기에는 Amazon EC2 인스턴스 AWS 리전 가 상주하는 , AWS 계정및 보안 그룹 IDs 포함됩니다. 보안 그룹에서 최대 5개의 보안 그룹 ARN을 지정할 수 있습니다.

     보안 그룹에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 사용 설명서의 Amazon VPC로 파일 시스템 액세스 제어를 참조하세요.

   - `protocol`에 DataSync가 파일 시스템의 SVM에 액세스하는 데 사용하는 프로토콜을 구성합니다.

- NFS의 경우, 기본 구성을 사용할 수 있습니다.

  ```
  --protocol NFS={}
  ```

- SMB의 경우, SVM에 액세스할 수 있는 사용자 이름과 암호를 지정해야 합니다.

  ```
  --protocol SMB={User=smb-user,Password=smb-password}
  ```

3. 명령을 실행합니다.

   방금 생성한 위치를 보여주는 응답을 받게 됩니다.

   ```
   {
       "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
   abcdef01234567890"
   }
   ```

를 사용하여 다른 클라우드 스토리지로 또는 다른 클라우드 스토리지에서 전송 AWS DataSync

AWS DataSync를 사용하면 다른 클라우드 공급자와 AWS 스토리지 서비스 간에 데이터를 전송할 수 있습니다. 자세한 내용은 Where can I transfer my data with DataSync? 섹션을 참조하세요.

주제

- 타사 클라우드 스토리지 시스템과 전송 계획
- Google Cloud Storage를 사용하여 AWS DataSync 전송 구성
- Microsoft Azure Blob Storage를 사용하여 전송 구성
- Microsoft Azure Files SMB 공유를 사용하여 AWS DataSync 전송 구성
- 다른 클라우드 객체 스토리지를 사용한 전송 구성

타사 클라우드 스토리지 시스템과 전송 계획

클라우드 간 데이터 전송을 계획할 때는 다음 사항을 고려하세요.

- 에이전트 사용: 에이전트는 기본 모드 작업을 사용할 때 다른 클라우드의 스토리지에 액세스하기 위해서만 필요합니다. 확장 모드 작업에는 에이전트가 필요하지 않습니다. 에이전트를 사용하기로 결정한 경우 클라우드 공급자의 S3 호환 객체 스토리지에서 전송 시 Amazon EC2 인스턴스로서 배포

할 수 있으며, 해당 특정 스토리지 서비스에서 전송 시 Google Compute Engine 또는 Azure Virtual Machine으로 각각 배포할 수 있습니다. Google 및 Azure의 파일 시스템에서 전송 시 에이전트를 Google 또는 Azure VM으로 배포하여 에이전트를 파일 시스템에 최대한 가까이 두는 것이 좋습니다. 또한 DataSync는 에이전트의 데이터를 로 압축 AWS하므로 송신 비용을 줄이는 데 도움이 될 수 있습니다. DataSync는 필요한 Amazon S3 API 호환성을 제공하는 검증된 클라우드 위치 목록을 제공합니다.

- 다른 클라우드의 객체 스토리지 엔드포인트: 타사 클라우드 공급자의 스토리지 엔드포인트는 일반적으로 리전 또는 계정별로 다릅니다. 리전 엔드포인트는 지정된 버킷 이름과 함께 DataSync 객체 스토리지 위치의 서버로 사용됩니다.
- 소스 객체의 스토리지 클래스: Amazon S3와 마찬가지로 일부 클라우드 공급자는 아카이브 계층을 지원하며, 아카이브된 객체에 액세스하려면 먼저 복원을 거쳐야 합니다. 예를 들어 Azure Blob 아카이브 계층의 객체는 데이터 전송 전에 표준 액세스를 위해 검색해야 합니다. Google Cloud Storage 아카이브 계층의 객체는 즉시 액세스할 수 있고 복원이 필요하지 않지만, 아카이브 계층에 직접 액세스할 경우 검색 비용이 발생합니다. 데이터 전송을 시작하기 전에 클라우드 간 스토리지 클래스 설명서를 검토하여 액세스 요구 사항 및 검색 요금을 확인합니다. Amazon S3에 아카이브된 객체를 복원하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 아카이브된 객체 복원을 참조하세요.
- 객체 스토리지 액세스: 타사 클라우드 공급자 간에 데이터를 전송하려면 인증 키 형태로 다른 클라우드의 객체 스토리지에 액세스해야 합니다. 예를 들어 Google Cloud Storage에 대한 액세스를 제공하려면 DataSync 객체 스토리지 위치를 구성하여, Google Cloud Storage XML API에 연결하고, 서비스 계정에 대한 해시 기반 메시지 인증 코드(HMAC) 키를 사용하여 인증합니다. Azure Blob 스토리지의 경우, 전용 Azure Blob DataSync 위치를 구성하여 SAS 토큰을 사용하여 인증합니다. DataSync는 AWS Secrets Manager 를 사용하여 객체 스토리지 자격 증명을 안전하게 저장합니다. 자세한 내용은 스토리지 위치 자격 증명 생성을 참조하세요.
- 객체 태그 지원:
  - Amazon S3와 달리, 모든 클라우드 공급자가 객체 태그를 지원하지는 않습니다. 클라우드 공급자가 Amazon S3 API를 통해 객체 태그를 지원하지 않거나 제공한 자격 증명이 태그를 검색하기에 충분하지 않은 경우, 소스 위치에서 태그를 읽으려고 시도하는 과정에서 DataSync 작업이 실패할 수 있습니다. 객체 태그를 지원하지 않거나 사용자가 태그를 유지하지 않으려는 경우 DataSync는 전송 중에 객체 태그 읽기 및 복사를 비활성화할 수 있는 작업 옵션을 제공합니다. 클라우드 공급자 설명서를 검토하여 객체 태그가 지원되는지 확인하고 전송을 시작하기 전에 전송 작업의 객체 태그 설정을 확인합니다.
  - Amazon S3 API를 사용하여 클라우드 공급자가 `get-object-tagging` 요청을 반환하는지 확인할 수 있습니다. 자세한 내용은 AWS CLI 명령 레퍼런스의 get-object-tagging을 참조하세요.

    객체 태그를 지원하는 클라우드 공급자는 다음 예시와 유사한 응답을 반환합니다.

```
aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint- url=https://
BUCKET_ENDPOINT --key prefix/file1

{

    "TagSet": []

}
```

`get-object-tagging`을 지원하지 않는 클라우드 공급자는 다음 메시지를 반환합니다.

```
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
```

- 요청 및 데이터 송신 관련 비용: 클라우드 객체 스토리지에서 데이터 전송 시, 데이터 읽기 및 데이터 전송과 관련된 요청 및 송신 비용이 발생합니다. 요청 요금은 클라우드 공급자별로 다르며, 해당하는 경우 스토리지 클래스별로 다릅니다. 읽으려는 스토리지 클래스와 관련된 요청의 특정 비용에 대해서는 클라우드 공급자 설명서를 참조하세요. DataSync가 데이터 전송에 부과하는 요청 요금에 대한 개요는 DataSync 사용 시 S3 요청 비용 평가 및 AWS DataSync 요금을 참조하세요. 특정 클라우드 공급자에게서 데이터를 전송하면 송신 요금이 발생합니다. 데이터 전송 비용은 클라우드 공급자마다 다르며 데이터가 저장되는 리전에 따라 달라집니다.
- 객체 스토리지 요청 속도: 클라우드 공급자는 객체 스토리지 플랫폼에 대해 다양한 성능 및 요청 속도 특성을 가집니다. 다른 클라우드 공급자의 요청 속도를 검토하고 요청 제한이 어디에 적용되는지 확인합니다. 여러 에이전트로 구성된 고도로 병렬화된 전송을 미리 계획할 때 특정 파티셔닝 또는 성능 향상이 필요할 수 있다는 점을 고려합니다.

  Amazon S3에는 솔루션 구축 시 참고할 수 있는 요청 속도가 문서화되어 제공됩니다. Amazon S3 요청 속도는 파티셔닝된 접두사별로 적용되며, 여러 접두사에 걸쳐 확장 가능합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 모범 사례 설계 패턴: Amazon S3 성능 최적화를 참조하세요.

Google Cloud Storage를 사용하여 AWS DataSync 전송 구성

를 사용하면 Google Cloud Storage와 다음 AWS 스토리지 서비스 간에 데이터를 전송할 AWS DataSync수 있습니다.

- Amazon S3
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP

전송 설정을 시작하려면 Google Cloud Storage의 위치를 생성합니다. 이 위치를 전송의 소스 또는 대상으로 사용할 수 있습니다. DataSync 에이전트는 Google Cloud Storage와 Amazon EFS 간에, 또는 Amazon FSx 간에 데이터를 전송하는 경우나 기본 모드 작업을 사용하는 경우에만 필요합니다. Google Cloud Storage와 Amazon S3 간 확장 모드 데이터 전송에는 에이전트가 필요하지 않습니다.

> **Note**
>
> Google Cloud Storage와 간의 프라이빗 클라우드 연결을 위해 에이전트와 함께 기본 모드를 AWS사용합니다.

개요

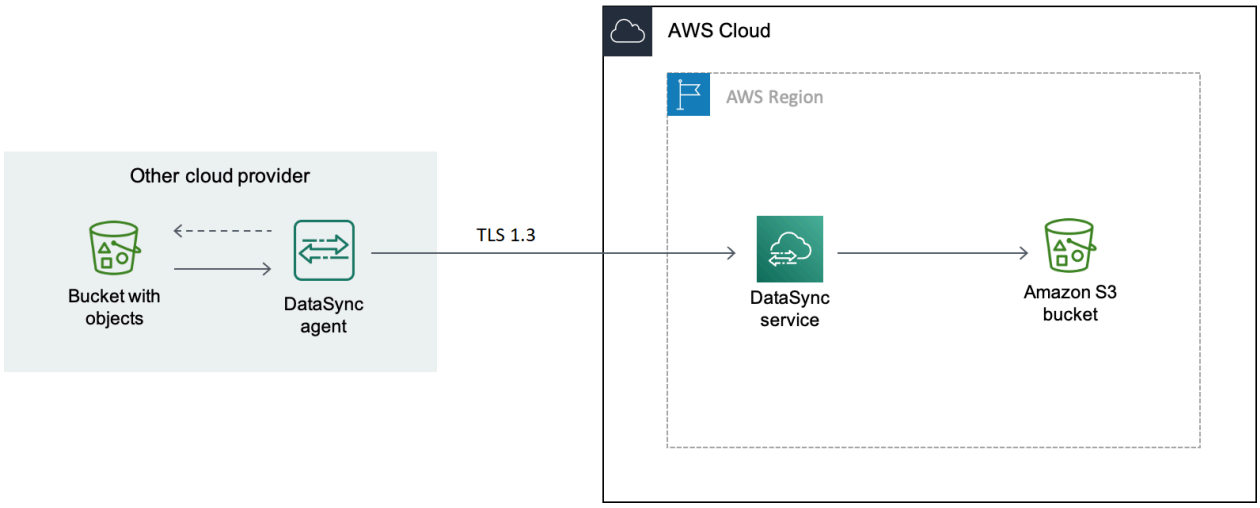
DataSync는 데이터 전송에 Google Cloud Storage XML API를 사용합니다. 이 API는 Google Cloud Storage 버킷을 사용하여 데이터를 읽고 쓸 수 있는 Amazon S3 호환 인터페이스를 제공합니다.

전송에 기본 모드를 사용하는 경우 Google Cloud Storage 또는 Amazon VPC에 에이전트를 배포할 수 있습니다.

Agent in Google Cloud

1. Google Cloud 환경에 DataSync 에이전트를 배포합니다.
2. 에이전트는 해시 기반 메시지 인증 코드(HMAC) 키를 사용하여 Google Cloud Storage 버킷을 읽습니다.
3. Google Cloud Storage 버킷의 객체는 퍼블릭 엔드포인트를 사용하여 TLS 1.3 AWS 클라우드 을 통해 로 안전하게 전송됩니다.
4. DataSync 서비스는 S3 버킷에 데이터를 씁니다.

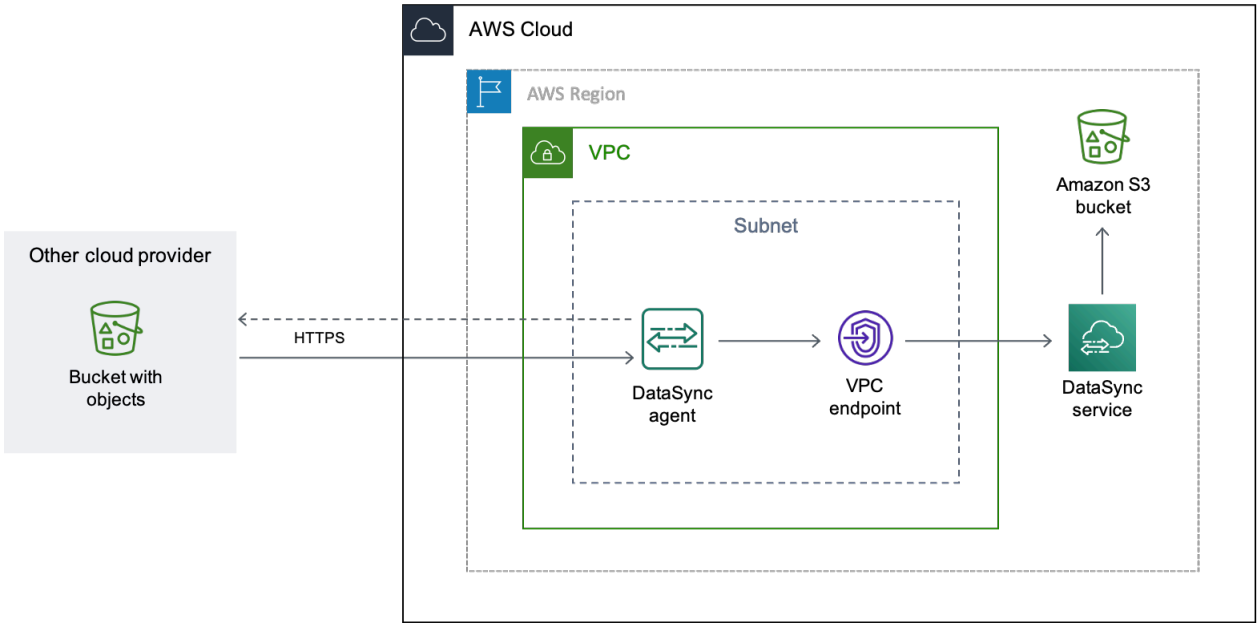
다음 다이어그램에서 전송을 보여 줍니다.



Agent in your VPC

1. DataSync 에이전트를 사용자 AWS 환경의 Virtual Private Cloud(VPC)에 배포합니다.
2. 에이전트는 해시 기반 메시지 인증 코드(HMAC) 키를 사용하여 Google Cloud Storage 버킷을 읽습니다.
3. Google Cloud Storage 버킷의 객체는 프라이빗 VPC 엔드포인트를 사용하여 TLS 1.3 AWS 클라우드 을 통해 로 안전하게 전송됩니다.
4. DataSync 서비스는 S3 버킷에 데이터를 씁니다.

다음 다이어그램에서 전송을 보여 줍니다.



비용

이 마이그레이션과 관련된 수수료에는 다음이 포함됩니다.

- Google 컴퓨팅 엔진 가상 머신 인스턴스 실행(Google 클라우드에 사용자 DataSync 에이전트를 배포하는 경우)
- Amazon EC2 인스턴스 실행(사용자 DataSync 에이전트를 AWS내부 VPC에 배포하는 경우)
- DataSync를 사용하여 데이터 전송. 여기에는 Google Cloud Storage 및 Amazon S3와 관련된 요청 요금이 포함됩니다(S3가 사용자 전송 위치인 경우)
- Google Cloud Storage 밖으로 데이터 전송
- Amazon S3에 데이터 저장

사전 조건

아직 다음 사항을 수행하지 않았다면 시작하기 전에 이를 수행합니다.

- AWS(으)로 전송하려는 객체가 포함된 Google Cloud Storage 버킷을 생성합니다.
- AWS 계정에 로그인 합니다
- 객체가 AWS에 들어오면 저장할 수 있는 Amazon S3 버킷을 생성합니다.

Google Cloud Storage 버킷에 HMAC 키 생성

DataSync는 Google 서비스 계정과 연결된 HMAC 키를 사용하여 데이터를 전송하는 버킷을 인증하고 이를 읽습니다. (HMAC 키를 만드는 방법에 대한 자세한 지침은 Google Cloud Storage 설명서를 참조하세요.)

HMAC 키 생성

1. Google 서비스 계정용 HMAC 키를 만드세요.
2. Google 서비스 계정에 최소한 `Storage Object Viewer`권한이 있는지 확인하세요.
3. HMAC 키 액세스 ID와 비밀 번호를 안전한 위치에 저장합니다.

   이러한 항목은 나중에 DataSync 소스 위치를 구성하는 데 필요합니다.

2단계: 사용자 네트워크 구성

네트워크 구성은 전송 시 DataSync 에이전트를 사용하는 경우에만 필요합니다. 마이그레이션에 필요한 네트워크 요구 사항은 사용자가 선택한 에이전트 배포 위치에 따라 달라집니다.

구글 클라우드의 DataSync 에이전트의 경우

Google Cloud에서 DataSync 에이전트를 호스팅하려면 DataSync가 퍼블릭 엔드포인트를 통해 전송을 할 수 있도록 네트워크를 구성합니다.

VPC의 DataSync 에이전트용

에이전트를 호스팅하려면 인터페이스 엔드포인트가 있는 VPC가 AWS필요합니다. DataSync는 VPC 엔드포인트를 사용하여 전송을 용이하게 합니다.

VPC 엔드포인트에 맞게 네트워크를 구성하려면

1. VPC가 없는 경우 S3 버킷 AWS 리전 과 동일한에 VPC를 생성합니다.
2. VPC용 프라이빗 서브넷을 생성합니다.
3. DataSync에 대한 VPC 엔드포인트를 생성합니다.
4. DataSync가 VPC 서비스 엔드포인트를 통해 전송을 허용하도록 사용자 네트워크를 구성합니다.

   이렇게 하려면 VPC 서비스 엔드포인트와 연결된 보안 그룹을 수정합니다.

3단계: DataSync 에이전트 생성(선택 사항)

DataSync 에이전트는 기본 모드 작업을 사용할 때만 필요합니다. 확장 모드를 사용하여 GCS(Google Cloud Storage)와 Amazon S3 간에 전송하는 경우 에이전트가 필요하지 않습니다. 기본 모드를 사용하려면 GCS 버킷에 액세스할 수 있는 DataSync 에이전트가 필요합니다.

Google Cloud의 경우

이 시나리오에서 DataSync 에이전트는 Google Cloud 환경에서 실행됩니다.

시작하기 전: Google 클라우드 CLI를 설치합니다.

Google 클라우드용 에이전트를 생성하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택한 다음, 에이전트 생성을 선택합니다.

3. 하이퍼바이저의 경우 VMware ESXi를 선택한 다음 이미지 다운로드를 선택하여 에이전트가 포함된 `.zip` 파일을 다운로드합니다.
4. 터미널을 엽니다. 다음 명령을 실행하여 이미지의 압축을 풉니다.

```
unzip AWS-DataSync-Agent-VMWare.zip
```

5. 다음 명령을 실행하여 `aws-datasync`로 시작하는 에이전트 `.ova`파일의 내용을 추출합니다.

```
tar -xvf aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt.ova
```

6. 다음 Google Cloud CLI 명령어를 실행하여 에이전트의 `.vmdk`파일을 Google Cloud로 가져옵니다.

```
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**
>
> `.vmdk`파일을 가져오는 데 최대 2시간이 걸릴 수 있습니다.

7. 방금 가져온 에이전트 이미지의 VM 인스턴스를 만들고 시작합니다.

   인스턴스에는 다음과 같은 에이전트 구성이 필요합니다. (인스턴스를 만드는 방법에 대한 자세한 지침은 Google Cloud Compute Engine 설명서를 참조하세요.)

   - 머신 유형은 다음 중 하나를 선택합니다.
     - e2-standard-8 - 최대 2천만 개의 객체를 처리하는 DataSync 작업 실행.
     - e2-standard-16 - 2천만 개 이상의 객체를 처리하는 DataSync 작업 실행.
   - 부팅 디스크 설정은 커스텀 이미지 섹션으로 갑니다. 그런 다음 방금 가져온 DataSync 에이전트 이미지를 선택합니다.
   - 서비스 계정 설정에서 Google 서비스 계정(1단계에서 사용한(와)과 동일한 계정)을 선택합니다.
   - 방화벽 설정에서 HTTP(포트 80) 트래픽을 허용하는 옵션을 선택합니다.

     DataSync 에이전트를 활성화하려면 에이전트에 포트 80이 열려 있어야 합니다. 이 포트는 공개적으로 액세스 되지 않아도 됩니다. 활성화되면 DataSync는 포트를 닫습니다.
8. VM 인스턴스를 실행한 후 해당 퍼블릭 IP 주소를 메모해 둡니다.

에이전트를 활성화하려면 이 IP 주소가 필요합니다.

9. DataSync 콘솔로 되돌아 갑니다. 에이전트 이미지를 다운로드한 에이전트 생성 화면에서 다음을 수행하여 에이전트를 활성화합니다.

   - 엔드포인트 유형에서 공용 서비스 엔드포인트 옵션(예: 미국 동부 오하이오의 공공 서비스 엔드포인트)을 선택합니다.
   - 활성화 키서 에이전트로부터 자동으로 활성화 키 받기를 선택합니다.
   - 에이전트 주소에는 방금 생성한 에이전트 VM 인스턴스의 퍼블릭 IP 주소를 입력합니다.
   - Get key를 선택합니다.

10. 에이전트 이름을 입력한 다음 에이전트 생성을 선택합니다.

에이전트가 온라인 상태이며 데이터를 전송할 준비가 되어 있습니다.

VPC의 경우

이 시나리오에서 에이전트는와 연결된 VPC에서 Amazon EC2 인스턴스로 실행됩니다 AWS 계정.

시작하기 전:(AWS Command Line InterfaceAWS CLI)를 설정하세요.

VPC용 에이전트를 만들려면

1. 터미널을 엽니다. S3 버킷과 연결된 계정을 사용하도록 AWS CLI 프로필을 구성해야 합니다.
2. 다음 명령을 복사합니다. *vpc-region*을 사용자 VPC가 있는 AWS 리전 로 바꿉니다(예, `us-east-1`).

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

3. 명령을 실행합니다. 출력에 표시된 `"Value"`속성을 메모해 둡니다.

   이 값은 사용자가 지정한 리전의 DataSync Amazon Machine Image(AMI) ID입니다. 예를 들어 AMI ID는 `ami-1234567890abcdef0`과 같을 수 있습니다.

4. 다음 URL을 복사합니다. 다시 한번, *vpc-region*을 사용자 VPC가 있는 AWS 리전 로 바꿉니다. *ami-id*을 이전 단계에서 기록한 AMI ID로 바꿉니다.

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

5. 브라우저에 URL을 붙여 넣습니다.

의 Amazon EC2 인스턴스 시작 페이지가 AWS Management Console 표시됩니다.

6. 인스턴스 유형에서 DataSync 에이전트용 권장 Amazon EC2 인스턴스 중 하나를 선택합니다.
7. 키 페어 이름에서 기존 키 페어를 선택하거나 새 이름을 생성합니다.
8. 네트워크 설정에서 에이전트를 배포하려는 VPC와 서브넷을 선택합니다.
9. 인스턴스 시작을 선택합니다.
10. Amazon EC2 인스턴스가 실행되면 VPC 엔드포인트를 선택합니다.
11. 에이전트 활성화.

4단계: Google Cloud Storag 버킷에 DataSync 소스 위치 생성

Google Cloud Storage 버킷의 DataSync 위치를 설정하려면 1단계에서 생성한 HMAC 키의 액세스 ID와 비밀번호가 필요합니다.

DataSync 소스 위치를 만들려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 객체 스토리지를 선택합니다.
4. 서버에 **`storage.googleapis.com`**를 입력합니다.
5. 버킷 이름에 Google Cloud Storage 버킷의 이름을 입력합니다.
6. 폴더에는 객체 접두사를 입력합니다.

   DataSync는 이 접두사가 있는 객체만 복사합니다.
7. 전송에 에이전트가 필요한 경우 에이전트 사용을 선택한 다음 3단계에서 생성한 에이전트를 선택합니다.
8. 추가 설정을 펼니다. 서버 프로토콜에서 HTTPS를 선택합니다. 서버 포트에서 443을 선택합니다.
9. 인증 섹션까지 아래로 스크롤합니다. 자격 증명 필요 확인란이 선택되어 있는지 확인하고 다음을 수행하세요.

   - 액세스 키에 사용자 HMAC 키의 액세스 ID를 입력합니다.
   - 비밀 키에 HMAC 키의 비밀 키를 직접 입력하거나 키가 포함된 AWS Secrets Manager 비밀을 지정합니다. 자세한 내용은 스토리지 위치에 대한 자격 증명 제공을 참조하세요.
10. 위치 생성을 선택합니다.

5단계: S3 버킷용 DataSync 대상 위치 생성

데이터가 최종적으로 가야 할 DataSync 위치가 필요합니다.

DataSync 대상 위치를 만들려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼쳐서 위치와 위치 생성을 선택합니다.
3. S3 버킷의 DataSync 위치를 생성합니다.

   VPC에 DataSync 에이전트를 배포한 경우이 자습서에서는 S3 버킷이 VPC 및 DataSync 에이전트 AWS 리전 와 동일한에 있다고 가정합니다.

6단계: DataSync 작업 생성 및 시작

소스 및 대상 위치가 구성된 상태에서 데이터를 이동할 수 있습니다 AWS.

DataSync 작업을 생성하고 시작하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 소스 위치 구성 페이지에서 다음 작업을 수행하세요.
   a. 기존 위치 선택을 선택합니다.
   b. 4단계에서 생성한 소스 위치를 선택한 후 다음을 선택합니다.
4. 대상 위치 구성 페이지에서 다음 작업을 수행하세요.
   a. 기존 위치 선택을 선택합니다.
   b. 5단계에서 생성한 대상 위치를 선택한 후 다음을 선택합니다.
5. 설정 구성 페이지에서 다음을 수행합니다.
   a. 데이터 전송 구성에서 추가 설정을 펼쳐서 개체 태그 복사 확인란의 선택을 취소합니다.

> **Important**
>
> Google Cloud Storage XML API는 객체 태그 읽기 또는 쓰기를 지원하지 않으므로 객체 태그 복사 시 DataSync 작업이 실패할 수 있습니다.

b. 원하는 다른 작업 설정을 구성한 후 다음을 선택합니다.

6. 검토 페이지에서 설정을 검토한 다음 작업 생성을 선택합니다.
7. 작업의 세부 정보 페이지에서 시작을 선택하고 다음 중 하나를 선택하세요:

   - 수정하지 않고 작업을 실행하려면 기본값으로 시작을 선택합니다.
   - 작업을 실행하기 전에 수정하려면 재정의 옵션으로 시작을 선택합니다.

작업이 완료되면 Google Cloud Storage 버킷의 객체가 S3 버킷에 있음을 확인할 수 있습니다.

Microsoft Azure Blob Storage를 사용하여 전송 구성

를 사용하면 Microsoft Azure Blob Storage (Azure Data Lake Storage Gen2Blob 스토리지 포함)와 다음 AWS 스토리지 서비스 간에 데이터를 전송할 AWS DataSync수 있습니다.

- Amazon S3
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP

이러한 종류의 전송을 설정하려면 Azure Blob Storage의 위치를 생성해야 합니다. 이 위치를 전송의 소스 또는 대상으로 사용할 수 있습니다. DataSync 에이전트는 Azure Blob과 Amazon EFS 또는 Amazon FSx 간에 데이터를 전송하거나 기본 모드 작업을 사용할 때만 필요합니다. 확장 모드를 사용하여 Azure Blob과 Amazon S3 간에 데이터를 전송하는 데는 에이전트가 필요하지 않습니다.

DataSync에 Azure Blob Storage 액세스 권한 제공

DataSync가 귀하의 Azure Blob Storage에 액세스하는 방법은 Blob 스토리지로 전송하는지 또는 Blob 스토리지에서 전송하는지 여부, 사용 중인 공유 액세스 서명(SAS) 토큰 의 종류 등 여러 요인에 따라 달라집니다. 또한 객체는 DataSync가 사용할 수 있는 액세스 티어에 속해야 합니다.

주제

- SAS 토큰
- 액세스 티어

SAS 토큰

SAS 토큰은 Blob 스토리지에 대한 액세스 권한을 지정합니다. (SAS에 대한 자세한 설명은 Azure Blob Storage설명서를 참조하십시오.)

SAS 토큰을 생성하여 다양한 수준의 액세스를 제공할 수 있습니다. DataSync는 다음과 같은 액세스 수준의 토큰을 지원합니다.

- Account
- 컨테이너

DataSync에 필요한 액세스 권한은 토큰의 범위에 따라 달라집니다. 올바른 권한이 없으면 전송이 실패할 수 있습니다. 예컨대, 태그가 있는 객체를 Azure Blob Storage로 이동하는데 SAS 토큰에 태그 권한이 없는 경우, 전송이 성공하지 못합니다.

주제

- 계정 수준 액세스를 위한 SAS 토큰 권한
- 컨테이너 수준 액세스를 위한 SAS 토큰 권한
- SAS 만료 정책

계정 수준 액세스를 위한 SAS 토큰 권한

DataSync에는 다음과 같은 권한이 있는 계정 수준 액세스 토큰이 필요합니다(Azure Blob Storage로 전송 또는 로부터의 수신 여부에 따라 다름).

Transfers from blob storage

- 허용된 서비스 - Blob
- 허용된 리소스 타입 - 컨테이너, 개체

  이러한 권한을 포함하지 않으면 DataSync는 객체 태그를 포함한 객체 메타데이터를 전송할 수 없습니다.
- 허용된 권한 - 읽기, 목록
- 허용된 Blob 인덱스 권한 - 읽기/쓰기(DataSync가 객체 태그를 복제하도록 하려는 경우)

Transfers to blob storage

- 허용된 서비스 - Blob
- 허용된 리소스 타입 - 컨테이너, 개체

  이러한 권한을 포함하지 않으면 DataSync는 객체 태그를 포함한 객체 메타데이터를 전송할 수 없습니다.
- 허용된 권한 - 읽기, 쓰기, 열거, 삭제(DataSync가 전송 소스에 없는 파일을 제거하도록 하려는 경우)
- 허용된 Blob 인덱스 권한 - 읽기/쓰기(DataSync가 객체 태그를 복제하도록 하려는 경우)

컨테이너 수준 액세스를 위한 SAS 토큰 권한

DataSync에는 다음과 같은 권한이 있는 컨테이너 수준 액세스 토큰이 필요합니다(Azure Blob Storage로 전송 또는 로부터의 수신 여부에 따라 다름).

Transfers from blob storage

- 읽기
- List
- 태그(DataSync가 객체 태그를 복제하도록 하려는 경우)

> **Note**
>
> Azure 포털에서 SAS 토큰을 생성할 때는 태그 권한을 추가할 수 없습니다. 태그 권한을 추가하려면 대신 Azure Storage Explorer앱을 사용하여 토큰을 생성하거나 계정 수준 액세스를 제공하는 SAS 토큰을 생성하세요.

Transfers to blob storage

- 읽기
- 쓰기
- List
- 삭제(DataSync가 전송 소스에 없는 파일을 제거하도록 하려는 경우)
- 태그(DataSync가 객체 태그를 복제하도록 하려는 경우)

> **Note**
>
> Azure 포털에서 SAS 토큰을 생성할 때는 태그 권한을 추가할 수 없습니다. 태그 권한을 추가하려면 대신 Azure Storage Explorer앱을 사용하여 토큰을 생성하거나 계정 수준 액세스를 제공하는 SAS 토큰을 생성하세요.

SAS 만료 정책

전송을 완료하기 전에 SAS가 만료되지 않도록 하세요. SAS 만료 정책 구성에 대한 자세한 설명은 Azure Blob Storage설명서를 참조하세요.

전송 중에 SAS가 만료되면 DataSync는 더 이상 귀하의 Azure Blob Storage위치에 액세스할 수 없습니다. (디렉터리 열기 실패 오류가 표시될 수 있습니다.) 이 경우, 새 SAS 토큰으로 위치를 업데이트하고 DataSync 작업을 다시 시작하세요.

액세스 티어

Azure Blob Storage로부터 전송할 때 DataSync는 핫 티어와 쿨 티어의 객체를 복사할 수 있습니다. 아카이브 액세스 티어에 있는 객체의 경우, 복제하려면 먼저 해당 객체를 핫 또는 쿨 계층으로 다시 하이드레이션해야 합니다.

Azure Blob Storage로 전송할 때 DataSync는 객체를 핫, 쿨 및 아카이브 액세스 티어으로 복제할 수 있습니다. 아카이브 액세스 티어에 객체를 복제하는 경우, 목적지의 모든 데이터를 확인하려는 경우, DataSync에서 전송을 확인할 수 없습니다.

DataSync는 콜드 액세스 티어를 지원하지 않습니다. 액세스 티어에 대한 자세한 설명은 Azure Blob Storage설명서를 참조하세요.

Azure Blob Storage전송 관련 고려 사항

DataSync를 사용하여 데이터를 Azure Blob Storage와 주고받을 때 유의해야 할 몇 가지 사항이 있습니다.

주제

- 비용
- 블럽 타입
- AWS 리전 가용성

- 객체 태그 복사
- Amazon S3로 전송
- 전송 목적지의 디렉터리 삭제
- 제한 사항

비용

Azure Blob Storage과 주고 받는 데이터 이동과 관련된 수수료에는 다음이 포함될 수 있습니다.

- Azure 가상 머신(VM) 실행(Azure에서 DataSync 에이전트를 배포하는 경우)
- Amazon EC2 인스턴스 실행(DataSync 에이전트를 AWS내부 VPC에 배포하는 경우)
- DataSync를 사용하여 데이터 전송, Azure Blob Storage및 Amazon S3와 관련된 요청 요금 포함(S3가 전송 위치 중 하나인 경우)
- 데이터를 Azure Blob Storage내부 또는 외부로 전송
- DataSync에서 지원하는 AWS 스토리지 서비스에 데이터 저장

블럽 타입

DataSync가 블럽 타입으로 작동하는 방식은 Azure Blob Storage이 전송의 출처인가 또는 목적지인가에 의존합니다. 데이터를 Blob 스토리지로 이동할 때 DataSync가 전송하는 객체 또는 파일은 블록 블롭만 될 수 있습니다. Blob 스토리지 외부로 데이터를 이동할 때 DataSync는 블록을 전송하고, 페이징하고, 블롭을 추가할 수 있습니다.

Blob 타입에 대한 자세한 설명은 Azure Blob Storage설명서를 참조하십시오.

AWS 리전 가용성

DataSync에서AWS 리전 지원하는 모든 위치에서 Azure Blob Storage전송 위치를 생성할 수 있습니다.

객체 태그 복사

데이터를 Azure Blob Storage과 주고 받을 때 DataSync가 객체 태그를 보존하는 기능은 다음 요인에 의존합니다:

- 객체 태그의 크기 - DataSync는 태그가 2KB를 초과하는 객체를 전송할 수 없습니다.
- DataSync가 객체 태그를 복제하도록 구성되었는지 여부 - DataSync는 기본적으로 객체 태그를 복제합니다.

- Azure스토리지 계정에서 사용하는 네임스페이스 - DataSync는 Azure스토리지 계정이 플랫 네임스페이스를 사용하는 경우, 객체 태그를 복제할 수 있지만, 계정이 계층적 네임스페이스 를 사용하는 경우에는 복제할 수 없습니다(Azure Data Lake Storage Gen2의 기능) . 스토리지 계정이 계층적 네임스페이스를 사용하고 객체 태그를 복제하려고 하면 DataSync 작업이 실패합니다.
- SAS 토큰이 태깅을 승인하는지 여부 - 객체 태그를 복제하는 데 필요한 권한은 토큰이 제공하는 액세스 수준에 따라 다릅니다. 객체 태그를 복제하려고 하는데 토큰에 태깅을 위한 적절한 권한이 없는 경우, 작업이 실패합니다. 자세한 설명은 계정 수준 액세스 토큰 또는 컨테이너 수준 액세스 토큰에 대한 권한 요건을 확인하세요.

Amazon S3로 전송

Amazon S3로 전송할 때 DataSync는 5TB보다 큰 객체 또는 2KB보다 큰 메타데이터가 있는 Azure Blob Storage객체를 전송하지 않습니다.

전송 목적지의 디렉터리 삭제

Azure Blob Storage로 전송할 때 DataSync는 전송 소스에 없는 Blob 스토리지의 객체를 제거할 수 있습니다. (DataSync 콘솔에서 삭제된 파일 유지 설정을 지우면 이 옵션을 구성할 수 있습니다. SAS 토큰에도 삭제 권한이 있어야 합니다.

이러한 방식으로 전송을 구성하면 Azure스토리지 계정이 계층적 네임스페이스를 사용하는 경우, DataSync는 Blob 스토리지의 디렉터리를 삭제하지 않습니다. 이 경우, Azure Storage Explorer를 사용하는 등의 방법으로 디렉터리를 수동으로 삭제해야 합니다.

제한 사항

Azure Blob Storage과 데이터를 주고 받을 때 다음과 같은 제한이 적용됩니다:

- DataSync는 전송을 용이하게 하기 위해 특정 위치에 일부 디렉터리를 생성합니다. Azure Blob Storage가 대상 위치이고 스토리지 계정에서 계층적 네임스페이스를 사용하는 경우, `/.aws-datasync` 폴더에 작업별 하위 디렉터리(예:`task-000011112222abcde`)가 있을 수 있습니다. DataSync는 일반적으로 전송 후 이러한 하위 디렉터리를 삭제합니다. 그렇지 않은 경우, 작업이 실행되지 않는 한 이러한 작업별 디렉터리를 직접 삭제할 수 있습니다.
- DataSync는 SAS 토큰을 사용하여 Azure Blob Storage컨테이너의 특정 폴더에만 액세스하는 것을 지원하지 않습니다.
- Blob 스토리지에 액세스하기 위한 사용자 위임 SAS 토큰은 DataSync에 제공할 수 없습니다.

DataSync 에이전트 생성(선택 사항)

DataSync 에이전트는 Azure Blob과 Amazon EFS 또는 Amazon FSx 간에 데이터를 전송하거나 기본 모드 작업을 사용할 때만 필요합니다. 확장 모드를 사용하여 Azure Blob과 Amazon S3 간에 데이터를 전송하는 데는 에이전트가 필요하지 않습니다. 이 섹션에서는 에이전트를 배포하고 활성화하는 방법을 설명합니다.

> **Tip**
>
> Amazon EC2 인스턴스에 에이전트를 배포할 수 있지만 Microsoft Hyper-V에이전트를 사용하면 네트워크 지연 시간이 줄어들고 데이터 압축률이 높아질 수 있습니다.

Microsoft Hyper-V 에이전트

Microsoft Hyper-V이미지와 함께 DataSync 에이전트를 Azure에 직접 배포할 수 있습니다.

> **Tip**
>
> 계속하기 전에 Hyper-V 에이전트를 더 빠르게 Azure에 배포하는 데 도움이 될 수 있는 쉘 스크립트를 사용해 보세요. GitHub에서 자세한 정보를 얻고 코드를 다운로드할 수 있습니다. 스크립트를 사용하는 경우, 에이전트의 활성화 키 받기에 대한 섹션으로 건너뛸 수 있습니다.

주제

- 사전 조건
- 에이전트 다운로드 및 준비
- Azure에 에이전트 배포하기
- 에이전트의 활성화 키 받기
- 에이전트 활성화하기

사전 조건

DataSync 에이전트를 준비하고 Azure에 배포하려면 다음을 수행해야 합니다:

- 로컬 Hyper-V시스템에서 활성화합니다.

- PowerShell를 설치합니다(Hyper-V Module 포함).
- Azure CLI를 설치합니다.
- AzCopy을 설치합니다.

에이전트 다운로드 및 준비

DataSync 콘솔에서 에이전트를 다운로드합니다. 에이전트를 Azure에 배포하려면 먼저 고정 크기의 가상 하드 디스크(VHD) 로 변환해야 합니다. 자세한 설명은 Azure설명서를 참조하세요.

에이전트를 다운로드하고 준비하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택한 다음, 에에이전트 생성을 선택합니다.
3. 하이퍼바이저의 경우, Microsoft Hyper-V를 선택한 다음 이미지 다운로드를 선택합니다.

   에이전트는 `.vhdx`파일이 포함된 `.zip`파일로 다운로드합니다.
4. 로컬 시스템에서 `.vhdx`파일을 추출합니다.
5. PowerShell를 열고 다음 중 하나를 수행합니다.

   a. 다음 `Convert-VHD`cmdlet을 복제합니다.

   ```
   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. *`local-path-to-vhdx-file`*의 각 인스턴스를 로컬 기기의 `.vhdx`파일 위치로 바꿉니다.

   c. 명령을 실행합니다.

   에이전트는 이제 고정 크기의 VHD(`.vhd`파일 형식 포함) 가 되어 Azure에에 배포할 준비가 되었습니다.

Azure에 에이전트 배포하기

Azure에 DataSync 에이전트를 배포하는 작업에는 다음이 포함됩니다.

- Azure에서 관리 디스크 만들기

- 해당 관리 디스크에 에이전트 업로드
- Linux 가상 시스템에 관리 디스크 연결

에이전트를 Azure에 배포하려면

1. PowerShell에서 에이전트의 `.vhd`파일이 들어 있는 디렉터리로 이동합니다.
2. `ls`명령을 실행하고 `Length`값을 저장합니다(예:85899346432).

   이는 이미지를 보관할 관리 디스크를 만들 때 필요한 에이전트 이미지의 크기(바이트) 입니다.
3. 관리 디스크를 만들려면 다음과 같이 하세요:

   a. 다음 AzureCLI 명령을 복사합니다:

   ```
   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*을 관리 디스크의 이름으로 바꿉니다.

   c. *your-resource-group*을 스토리지 계정이 속한 Azure리소스 그룹의 명칭으로 바꾸세요.

   d. *your-azure-region*을 귀하의 리소스 그룹이 위치한 Azure리전으로 바꾸세요.

   e. *agent-size-bytes*을 귀하의 에이전트 이미지 크기로 바꾸세요.

   f. 명령을 실행합니다.

   이 명령을 실행하면 DataSync 에이전트를 업로드할 수 있는 표준 SKU가 포함된 빈 관리 디스크가 생성됩니다.
4. 관리 디스크에 대한 쓰기 액세스를 허용하는 공유 액세스 서명(SAS) 을 생성하려면 다음을 수행하세요.

   a. 다음 AzureCLI 명령을 복사합니다:

   ```
   az disk grant-access -n your-managed-disk `
   -g your-resource-group `
   --access-level Write `
   --duration-in-seconds 86400
   ```

b. *your-managed-disk*을 귀하가 생성한 관리 디스크의 명칭으로 바꿉니다.

c. *your-resource-group*을 스토리지 계정이 속한 Azure리소스 그룹의 명칭으로 바꾸세요.

d. 명령을 실행합니다.

출력에 표시된 SAS URI를 메모해 둡니다. 에이전트를 Azure에 업로드할 때 이 URI가 필요합니다.

SAS를 사용하면 디스크에 최대 1시간 동안 쓸 수 있습니다. 즉, 에이전트를 관리 디스크에 업로드하는 데 한 시간이 걸립니다.

5. 에이전트를 Azure의 관리 디스크에 업로드하려면 다음을 수행하세요:

a. 다음 AzCopy명령을 복사합니다:

```
.\azcopy copy local-path-to-vhd-file sas-uri --blob-type PageBlob
```

b. *local-path-to-vhd-file*을 귀하의 로컬 기기에서 에이전트 .vhd파일 위치로 바꾸세요.

c. *sas-uri*을 az disk grant-access명령을 실행할 때 받은 SAS URI로 바꾸세요.

d. 명령을 실행합니다.

6. 에이전트 업로드가 완료되면 관리 디스크에 대한 액세스 권한을 취소하세요. 그렇게 하려면 다음의 AzureCLI 명령을 복사합니다:

```
az disk revoke-access -n your-managed-disk -g your-resource-group
```

a. *your-resource-group*을 스토리지 계정이 속한 Azure리소스 그룹의 명칭으로 바꾸세요.

b. *your-managed-disk*을 귀하가 생성한 관리 디스크의 명칭으로 바꿉니다.

c. 명령을 실행합니다.

7. 관리 디스크를 새 LinuxVM에 연결하려면 다음을 수행하세요.

a. 다음 AzureCLI 명령을 복사합니다:

```
az vm create --resource-group your-resource-group `
--location eastus `
--name your-agent-vm `
--size Standard_E4as_v4 `
--os-type linux `
--attach-os-disk your-managed-disk
```

b. *your-resource-group*을 스토리지 계정이 속한 Azure리소스 그룹의 명칭으로 바꾸세요.

c. *your-agent-vm*을 귀하가 기억할 수 있는 VM 이름으로 바꾸세요.

d. *your-managed-disk*을 VM에 연결하는 관리 디스크의 이름으로 바꿉니다.

e. 명령을 실행합니다.

에이전트를 배포했습니다. 데이터 전송 구성을 시작하려면 먼저 에이전트를 활성화해야 합니다.

에이전트의 활성화 키 받기

DataSync 에이전트의 활성화 키를 수동으로 가져오려면 다음 단계를 따르세요.

또는 DataSync가 자동으로 활성화 키를 귀하에게 가져올 수도 있지만 이 접근 방식에는 일부 네트워크 구성이 필요합니다.

에이전트의 활성화 키를 받으려면

1. Azure포털에서 사용자 지정 스토리지 계정 활성화를 설정으로 선택하고 귀하의 Azure스토리지 계정을 지정하여 에이전트용 VM에 대한 부팅 진단을 활성화합니다.

   에이전트의 VM에 대한 부팅 진단을 활성화한 후 에이전트의 로컬 콘솔에 액세스하여 활성화 키를 가져올 수 있습니다.
2. Azure포털에 있는 동안 VM으로 이동하여 직렬 콘솔을 선택합니다.
3. 에이전트의 로컬 콘솔에서 다음 기본 자격 증명을 사용하여 로그인합니다.

   - 사용자 이름 – **admin**
   - 암호 – **password**

   어느 시점에서든 최소한 에이전트의 비밀번호는 변경하는 것이 좋습니다. 에이전트의 로컬 콘솔에서 기본 메뉴에 **5**를 입력한 다음 passwd명령을 사용하여 암호를 변경합니다.
4. 에이전트의 활성화 키를 가져오려면 **0**를 누르세요.
5. DataSync를 사용 중인 AWS 리전 를 입력합니다(예: **us-east-1**).
6. 에이전트가 연결하는 데 사용할 서비스 엔드포인트를 선택합니다 AWS.
7. `Activation key` 출력의 값을 저장합니다.

에이전트 활성화하기

활성화 키가 있으면 DataSync 에이전트 생성을 완료할 수 있습니다.

에이전트를 활성화하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택한 다음, 에에이전트 생성을 선택합니다.
3. 하이퍼바이저의 경우, Microsoft Hyper-V를 선택하세요.
4. 엔드포인트 타입의 경우, 에이전트의 활성화 키를 받을 때 지정한 것과 동일한 타입의 서비스 엔드포인트를 선택합니다(예: **##** 이름에서 공용 서비스 엔드포인트 선택).
5. 에이전트가 사용하는 서비스 엔드포인트 타입과 작동하도록 네트워크를 구성하세요. 서비스 엔드포인트 네트워크 요건은 다음 항목을 참조하세요:
   - VPC 엔드포인트
   - 퍼블릭 엔드포인트
   - Federal Information Processing Standard(FIPS) 엔드포인트
6. 활성화 키의 경우, 다음을 수행하세요:
   a. 에이전트의 활성화 키를 수동으로 입력합니다를 선택합니다.
   b. 에이전트의 로컬 콘솔에서 받은 활성화 키를 입력합니다.
7. Create agent(에이전트 생성)을 선택합니다.

에이전트가 귀하의 Azure Blob Storage과 연결할 준비가 되었습니다. 자세한 설명은 귀하의 Azure Blob Storage전송 위치 생성섹션을 참조하세요.

Amazon EC2 에에이전트

Amazon EC2 인스턴스에 DataSync 에이전트를 배포할 수 있습니다.

Amazon EC2 에이전트를 만들려면

1. Amazon EC2 에이전트를 배포합니다.
2. 에이전트가 AWS와 통신하는 데 사용하는 서비스 엔드포인트를 선택합니다.

   이 경우, Virtual Private Cloud(VPC) 서비스 엔드포인트를 사용하는 것이 좋습니다.
3. VPC 서비스엔드포인트 와 함께 작동하도록 네트워크를 구성합니다.

4. 에이전트를 활성화합니다.

귀하의 Azure Blob Storage전송 위치 생성

귀하의 Azure Blob Storage를 전송 소스 또는 목적지로 사용하도록 DataSync를 구성할 수 있습니다.

시작하기 전 준비 사항

DataSync가 액세스 티어 및 Blob 타입에 Azure Blob Storage액세스하고 이를 처리하는 방법을 알고 있어야 합니다. 귀하의 Azure Blob Storage컨테이너에 연결할 수 있는 DataSync 에이전트도 필요합니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 타입에서 Microsoft Azure Blob Storage를 선택합니다.
4. 컨테이너 URL에는 전송과 관련된 컨테이너의 URL을 입력합니다.
5. (옵션) 목적지로 사용되는 액세스 등급의 경우, 귀하의 객체 또는 파일들이 이전되기 바라는 액세스 등급을 선택합니다.
6. 전송을 컨테이너의 가상 디렉터리로만 제한하려면 폴더에 경로 세그먼트를 입력합니다(예: `/my/images`).
7. 전송에 에이전트가 필요한 경우 에이전트 사용을 선택한 다음 Azure Blob Storage 컨테이너에 연결할 수 있는 DataSync 에이전트를 선택합니다.
8. SAS 토큰의 경우 DataSync가 Blob 스토리지에 액세스하는 데 필요한 자격 증명을 제공합니다. Azure Blob 스토리지의 일부 퍼블릭 데이터세트에는 자격 증명이 필요하지 않습니다. SAS 토큰을 직접 입력하거나 토큰이 포함된 AWS Secrets Manager 보안 암호를 지정할 수 있습니다. 자세한 내용은 스토리지 위치에 대한 자격 증명 제공을 참조하세요.

   SAS 토큰은 스토리지 리소스 URI와 물음표(?) 다음에 오는 SAS URI 문자열의 일부입니다. 토큰은 다음과 같은 형태입니다:

   ```
   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. (옵션) 위치에 태그를 지정하려면 키 및 값 필드에 값을 입력합니다.

태그는 AWS 리소스를 관리, 필터링 및 검색하는 데 도움이 됩니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

10. 위치 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-location-azure-blob`명령을 복사합니다:

```
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. `--container-url`파라미터에는 전송에 관련된 Azure Blob Storage컨테이너의 URL을 지정합니다.
3. `--authentication-type` 파라미터에서 SAS를 지정합니다. 인증이 필요하지 않은 퍼블릭 데이터세트에 액세스하는 경우 NONE을 지정합니다.
4. `--sas-configuration`파라미터 Token옵션의 경우, DataSync가 Blob 스토리지에 액세스할 수 있도록 허용하는 SAS 토큰을 지정합니다.

   또한 AWS Secrets Manager를 사용하여 키를 보호하기 위한 추가 파라미터를 제공할 수 있습니다. 자세한 내용은 스토리지 위치에 대한 자격 증명 제공을 참조하세요.

   SAS 토큰은 스토리지 리소스 URI와 물음표(?) 다음에 오는 SAS URI 문자열의 일부입니다. 토큰은 다음과 같은 형태입니다:

```
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. (선택 사항) `--agent-arns` 파라미터에 컨테이너에 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)을 지정합니다.

다음은 에이전트 ARN의 예입니다: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

복수의 에이전트를 지정할 수 있습니다. 자세한 설명은 여러 DataSync 에이전트 사용섹션을 참조하세요.

6. `--subdirectory` 파라미터에 관하여, 컨테이너의 가상 디렉터리로 전송을 제한하려면 경로 세그먼트를 지정하세요(예:`/my/images`).
7. (옵션) `--access-tier`파라미터에 관하여, 귀하의 객체 또는 파일들이 이전되기 바라는 액세스 등급(`HOT`, `COOL`, 또는 `ARCHIVE`)을 선택합니다.

   이 파라미터는 이 위치를 전송 목적지로 사용하는 경우에만 적용됩니다.
8. (옵션) 위치를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 쌍을 `--tags`파라미터에 지정합니다.

   위치에 이름 태그를 생성하는 것이 좋습니다.
9. `create-location-azure-blob` 명령을 실행합니다.

   명령이 성공하면 생성한 위치의 ARN을 보여주는 응답을 받게 됩니다. 예제:

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh"
}
```

Azure Blob Storage전송 위치 보기

귀하의 Azure Blob Storage을 위한 기존 DataSync 전송 위치에 대한 세부 정보를 얻을 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 위치를 선택합니다.
3. Azure Blob Storage 위치를 선택합니다.

   위치를 사용하는 모든 DataSync 전송 작업을 포함하여 위치에 대한 세부 정보를 볼 수 있습니다.

사용 AWS CLI

1. 다음 `describe-location-azure-blob`명령을 복사합니다:

```
aws datasync describe-location-azure-blob \
  --location-arn "your-azure-blob-location-arn"
```

2. `--location-arn`파라미터에는 귀하가 생성한 Azure Blob Storage위치의 ARN(예:`arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`)을 지정합니다.
3. `describe-location-azure-blob` 명령을 실행합니다.

   위치에 대한 세부 정보를 보여주는 응답을 받게 됩니다. 예제:

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

Azure Blob Storage전송 위치 업데이트

필요한 경우, 콘솔에서 또는 AWS CLI를 사용하여 위치 구성을 수정할 수 있습니다.

사용 AWS CLI

1. 다음 `update-location-azure-blob`명령을 복사합니다:

```
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. `--location-arn`파라미터에는 업데이트하려는 Azure Blob Storage위치의 ARN을 지정합니다(예:`arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. `--authentication-type` 파라미터에서 SAS를 지정합니다.
4. `--sas-configuration`파라미터 Token옵션의 경우, DataSync가 Blob 스토리지에 액세스할 수 있도록 허용하는 SAS 토큰을 지정합니다.

   토큰은 스토리지 리소스 URI와 물음표(?) 다음에 오는 SAS URI 문자열의 일부입니다. 토큰은 다음과 같은 형태입니다:

   ```
   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. `--agent-arns`파라미터에는 컨테이너에 연결할 DataSync 에이전트의 Amazon 리소스 이름(ARN) 을 지정합니다.

   다음은 에이전트 ARN의 예입니다: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

   복수의 에이전트를 지정할 수 있습니다. 자세한 설명은 여러 DataSync 에이전트 사용섹션을 참조하세요.
6. `--subdirectory` 파라미터에 관하여, 컨테이너의 가상 디렉터리로 전송을 제한하려면 경로 세그먼트를 지정하세요(예:`/my/images`).
7. (옵션) `--access-tier`파라미터에 관하여 귀하의 객체 또는 파일들이 이전되기 바라는 액세스 등급(`HOT`, `COOL`, 또는 `ARCHIVE`)을 선택합니다.

   이 파라미터는 이 위치를 전송 목적지로 사용하는 경우에만 적용됩니다.

다음 단계

귀하의 Azure Blob Storage을 위한 DataSync 위치 생성을 완료한 후 전송 설정을 계속할 수 있습니다. 고려해야 할 몇 가지 단계는 다음과 같습니다.

1. 아직 만들지 않았다면 다른 위치를 만들어 데이터를 귀하의 Azure Blob Storage와 주고받을 수도 있습니다.

2. 특히 전송 위치에 유사한 메타데이터 구조가 없는 경우, DataSync가 메타데이터와 특수 파일을 처리하는 방법을 알아보세요.
3. 데이터 전송 방식을 구성하세요. 예컨대, Blob 스토리지에서 데이터의 일부만 전송하거나 소스 위치에 없는 파일을 삭제할 수 있습니다(SAS 토큰에 삭제 권한이 있는 한).
4. 전송을 시작하세요.

Microsoft Azure Files SMB 공유를 사용하여 AWS DataSync 전송 구성

Microsoft Azure Files 서버 메시지 블록(SMB) 공유에서 데이터를 전송 AWS DataSync 하도록를 구성할 수 있습니다.

> **Tip**
>
> Azure Files SMB 공유에서 로 데이터를 이동하는 방법에 대한 전체 연습은 AWS 스토리지 블로그를 AWS참조하세요.

DataSync에 SMB 공유 액세스 권한 제공

DataSync는 SMB 프로토콜을 사용하여 SMB 공유에 연결하고 사용자가 제공한 자격 증명으로 인증합니다.

주제

- 지원되는 SMB 프로토콜 버전
- 필수 권한

지원되는 SMB 프로토콜 버전

기본적으로 DataSync는 SMB 파일 서버와의 협상을 기반으로 SMB 프로토콜 버전을 자동으로 선택합니다.

특정 SMB 버전을 사용하도록 DataSync를 구성할 수도 있지만 DataSync가 SMB 파일 서버와 자동으로 협상하는 데 문제가 있는 경우에만 이렇게 하는 것이 좋습니다. DataSync는 SMB 버전 1.0 이상을 지원합니다. 보안상의 이유로 SMB 버전 3.0.2 이상을 사용하는 것이 좋습니다. SMB 1.0과 같은 이전 버전에는 알려진 보안 취약성이 포함되어 있어, 공격자가 데이터를 손상시키기 위해 이를 악용할 수 있습니다.

DataSync 콘솔 및 API의 옵션 목록은 다음 표를 참조하세요.

콘솔 옵션	API 옵션	설명
자동	`AUTOMATIC`	DataSync와 SMB 파일 서버는 2.1과 3.1.1 사이에서 상호 지원하는 SMB의 가장 높은 버전을 협상합니다. 이는 기본값이며 권장 옵션입니다. 대신 파일 서버에서 지원하지 않는 특정 버전을 선택하면 `Operation Not Supported` 오류가 발생할 수 있습니다.
SMB 3.0.2	`SMB3`	프로토콜 협상을 SMB 버전 3.0.2로만 제한합니다.
SMB 2.1	`SMB2`	프로토콜 협상을 SMB 버전 2.1로만 제한합니다.
SMB 2.0	`SMB2_0`	프로토콜 협상을 SMB 버전 2.0으로만 제한합니다.
SMB 1.0	`SMB1`	프로토콜 협상을 SMB 버전 1.0으로만 제한합니다.

필수 권한

DataSync에는 SMB 위치를 마운트하고 액세스할 수 있는 권한이 있는 사용자가 필요합니다. 이 사용자는 Windows File Server의 로컬 사용자이거나 Microsoft Active Directory에 정의된 도메인 사용자일 수 있습니다.

객체 소유권을 설정하려면 `SE_RESTORE_NAME`권한이 필요하며, 이 권한은 일반적으로 내장된 Active Directory 그룹 회원 백업 운영자 및 도메인 관리자에게 부여됩니다. 사용자에게 이 권한을 DataSync에 제공하면 NTFS 시스템 액세스 제어 목록(SACL)을 제외한 파일, 폴더 및 파일 메타데이터에 대한 충분한 권한을 보장하는 데도 도움이 됩니다.

SACL을 복사하려면 추가 권한이 필요합니다. 이 작업에는 특히 Windows `SE_SECURITY_NAME`권한이 필요하며, 이 권한은 Domain Admins 그룹의 멤버에게 부여됩니다. SACL을 복사하도록 태스크를 구성하는 경우, 사용자에게 필요한 권한이 있는지 확인해야 합니다. SACL을 복사하도록 작업을 구성하는 방법에 대한 자세한 내용은 파일, 객체 및 메타데이터 처리 방법 구성단원을 참조하세요.

SMB 파일 서버와 Amazon FSx for Windows File Server 파일 시스템 간에 데이터를 복사하는 경우 원본 및 대상 위치는 동일한 Microsoft Active Directory 도메인에 속하거나 해당 도메인 간에 Active Directory 신뢰 관계를 가져야 합니다.

콘솔을 사용하여 Azure File Transfer 위치 생성

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. Location type(위치 유형)에서 Server Message Block (SMB)(SMB(Server Message Block))을 선택합니다.

   나중에 이 위치를 소스 또는 대상 주소로서 구성합니다.
4. 에이전트의 경우 SMB 공유에 연결할 DataSync 에이전트를 하나 이상 선택합니다.

   에이전트를 두 개 이상 선택하는 경우 한 위치에 여러 에이전트를 사용하는 것을 이해해야 합니다.
5. SMB 서버의 경우 DataSync 에이전트가 마운트할 SMB 공유의 도메인 이름 시스템(DNS) 이름 또는 IP 주소를 입력합니다.

   > **Note**
   >
   > IP 버전 6(IPv6) 주소는 지정할 수 없습니다.

6. 공유 이름에는 DataSync가 데이터를 읽거나 쓸 SMB 공유에서 내보낸 공유의 이름을 입력합니다.

   공유 경로에 하위 디렉토리(예: `/path/to/subdirectory`)를 포함할 수 있습니다. 네트워크의 다른 SMB 클라이언트도 이 경로를 마운트할 수 있는지 확인하세요.

   하위 디렉터리의 모든 데이터를 복사하려면 DataSync가 SMB 공유를 마운트하고 모든 데이터에 액세스할 수 있어야 합니다. 자세한 설명은 필수 권한섹션을 참조하세요.
7. (선택 사항) 추가 설정을 확장하고 SMB 공유에 액세스할 때 DataSync에서 사용할 SMB 버전을 선택합니다.

   기본적으로 DataSync는 SMB 공유와의 협상을 기반으로 버전을 자동으로 선택합니다. 자세한 내용은 지원되는 SMB 버전을 참조하십시오.
8. 사용자에 SMB 공유를 마운트할 수 있고 전송과 관련된 파일 및 폴더에 액세스할 권한이 있는 사용자 이름을 입력합니다.

   자세한 설명은 필수 권한섹션을 참조하세요.
9. 암호에 귀하의 SMB 공유를 탑재할 수 있으며 전송에 관련된 파일과 폴더에 액세스할 수 있는 권한이 있는 사용자의 암호를 입력합니다.
10. (선택 사항) 도메인에는 SMB 공유가 속한 Windows 도메인 이름을 입력합니다.

환경에 여러 도메인이 있는 경우 이 설정을 구성하면 DataSync가 올바른 공유에 연결되도록 할 수 있습니다.

11. (선택 사항) 태그 추가를 선택하여 위치에 태그를 지정합니다.

    태그는 위치를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 쌍입니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

12. 위치 생성을 선택합니다.

다른 클라우드 객체 스토리지를 사용한 전송 구성

를 사용하면 AWS 스토리지 서비스와 다음 클라우드 객체 스토리지 공급자 간에 데이터를 전송할 AWS DataSync수 있습니다.

- 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

DataSync 에이전트는 다른 클라우드와 Amazon EFS 또는 Amazon FSx의 스토리지 시스템 간에 데이터를 전송하거나 기본 모드 작업을 사용할 때만 필요합니다. 확장 모드를 사용하면 에이전트가 다른 클라우드의 스토리지 시스템과 Amazon S3 간에 데이터를 전송할 필요가 없습니다.

에이전트 사용 여부와 관계없이 클라우드 객체 스토리지를 위한 전송 위치(특히 객체 스토리지 위치)를 생성해야 합니다. DataSync는 이 위치를 전송의 소스 또는 목적지로 사용할 수 있습니다.

DataSync에 다른 클라우드 객체 스토리지에 대한 액세스 권한 제공

DataSync가 클라우드 객체 스토리지에 액세스하는 방법은 스토리지가 Amazon S3 API와 호환되는지 여부, DataSync가 스토리지에 액세스하는 데 필요한 권한 및 보안 인증을 포함하는 여러 요인에 따라 달라집니다.

주제

- Amazon S3 API 호환성
- 스토리지 권한 및 엔드포인트
- 스토리지 보안 인증

Amazon S3 API 호환성

DataSync를 연결하려면 클라우드 객체 스토리지가 다음의 Amazon S3 API 작업과 호환되어야 합니다.

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

스토리지 권한 및 엔드포인트

DataSync가 클라우드 객체 스토리지에 액세스할 수 있도록 권한을 구성해야 합니다. 객체 스토리지가 소스 위치인 경우 DataSync에는 데이터를 전송하는 버킷에 대한 읽기 및 나열 권한이 필요합니다. 객체 스토리지가 대상 위치인 경우 DataSync에는 버킷에 대한 읽기, 나열, 쓰기, 삭제 권한이 필요합니다.

또한 DataSync에는 스토리지에 연결하기 위한 엔드포인트(또는 서버)가 필요합니다. 다음 표는 DataSync가 다른 클라우드 객체 스토리지에 액세스하는 데 사용할 수 있는 엔드포인트를 설명합니다.

기타 클라우드 제공업체	엔드포인트
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` (대부분의 리전)
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**
>
> 스토리지 엔드포인트에서 버킷 권한 및 업데이트된 정보를 구성하는 방법에 대한 자세한 내용은 클라우드 제공자의 설명서를 참조하세요.

스토리지 보안 인증

또한 DataSync에는 전송과 관련된 객체 스토리지 버킷에 액세스하기 위한 자격 증명 또한 필요합니다. 이는 클라우드 스토리지 공급자가 이러한 보안 인증을 참조하는 방식에 따라 액세스 키, 비밀 키 또는 이와 유사한 것일 수 있습니다.

자세한 내용은 클라우드 공급자의 설명서를 참조하세요.

다른 클라우드 개체 스토리지에서 전송할 때 고려할 사항

DataSync를 사용하여 다른 클라우드 스토리지 제공자로 또는 다른 클라우드 스토리지 제공자로부터 객체를 전송할 계획이라면 몇 가지 염두에 두어야 할 사항이 있습니다.

주제

- 비용
- 스토리지 클래스
- 객체 태그
- Amazon S3로 전송

비용

다른 클라우드 스토리지 제공업체에서 데이터를 주고받는 데 따르는 수수료에는 다음이 포함될 수 있습니다.

- DataSync 에이전트용 Amazon EC2 인스턴스 실행
- DataSync를 사용한 데이터 전송, 여기에는 클라우드 객체 스토리지 및 Amazon S3와 관련된 요청 요금이 포함됩니다(S3가 전송 목적지인 경우).
- 클라우드 스토리지 내부 또는 외부 데이터 전송(클라우드 제공업체 요금 확인)
- DataSync에서 지원하는 AWS 스토리지 서비스에 데이터 저장
- 다른 클라우드 공급자에 데이터 저장(클라우드 제공업체 가격 확인)

스토리지 클래스

일부 클라우드 스토리지 제공자에는(Amazon S3와 유사한) 스토리지 클래스가 있습니다. 이 클래스는 DataSync가 먼저 복원하지 않으면 읽을 수 없습니다. 예를 들어, Oracle Cloud Infrastructure Object Storage에는 아카이브 스토리지 클래스가 있습니다. DataSync에서 객체를 전송하려면 먼저 해당 스토리지 클래스의 객체를 복원해야 합니다. 자세한 내용은 클라우드 공급자의 문서를 참조하세요.

객체 태그

모든 클라우드 공급자가 객체 태그를 지원하지는 않습니다. 그런 경우 Amazon S3 API를 통한 태그 쿼리가 허용되지 않을 수 있습니다. 어떤 상황에서든 객체 태그를 복사하려고 하면 DataSync 전송 태스크가 실패할 수 있습니다.

태스크를 생성, 시작 또는 업데이트할 때 DataSync 콘솔에서 객체 태그 복사 확인란을 선택 해제하면 이러한 문제를 피할 수 있습니다.

Amazon S3로 전송

Amazon S3로 전송할 때 DataSync는 5TB보다 큰 객체를 전송할 수 없습니다. 또한 DataSync는 객체 메타데이터를 최대 2KB까지만 복사할 수 있습니다.

DataSync 에이전트 생성

DataSync 에이전트는 다른 클라우드와 Amazon EFS 또는 Amazon FSx의 스토리지 시스템 간에 데이터를 전송하거나 기본 모드 작업을 사용할 때만 필요합니다. 확장 모드를 사용하면 에이전트가 다른 클라우드의 스토리지 시스템과 Amazon S3 간에 데이터를 전송할 필요가 없습니다. 이 섹션에서는 AWS 가상 프라이빗 클라우드(VPC)의 Amazon EC2 인스턴스에 에이전트를 배포하고 활성화하는 방법을 설명합니다.

Amazon EC2 에이전트를 만들려면

1. Amazon EC2 에이전트를 배포합니다.
2. 에이전트가 통신하는 데 사용하는 서비스 엔드포인트를 선택합니다 AWS.

   이러한 경우 VPC 서비스 엔드포인트를 사용하는 것이 좋습니다.
3. VPC 서비스 엔드포인트와 함께 작동하도록 네트워크를 구성합니다.
4. 에이전트를 활성화합니다.

다른 클라우드 객체 스토리지를 위한 전송 위치 생성

클라우드 객체 스토리지를 소스 또는 대상 위치로서 사용하도록 DataSync를 구성할 수 있습니다.

시작하기 전 준비 사항

DataSync가 클라우드 객체 스토리지에 액세스하는 방법을 알고 있어야 합니다. 또한 클라우드 객체 스토리지에 연결할 수 있는 DataSync에이전트가 필요합니다.

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음, 위치와 위치 생성을 선택합니다.
3. 위치 유형에서 객체 스토리지를 선택합니다.
4. 서버의 경우 DataSync가 클라우드 객체 스토리지에 액세스하는 데 사용할 수 있는 엔드포인트를 입력합니다.

- 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`대부분의 리전)
- 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. 버킷 이름에는 데이터를 주고받는 객체 스토리지 버킷의 이름을 입력합니다.
6. 폴더에는 객체 접두사를 입력합니다. DataSync는 이 접두사가 있는 객체만 전송합니다.
7. 전송에 에이전트가 필요한 경우 에이전트 사용을 선택한 다음 클라우드 객체 스토리지에 연결할 수 있는 DataSync 에이전트를 선택합니다.
8. 추가 설정을 펼니다. 서버 프로토콜에서 HTTPS를 선택합니다. 서버 포트에서 443을 선택합니다.
9. 인증 섹션까지 아래로 스크롤합니다. 보안 인증 필요 확인란이 선택되어 있는지 확인한 다음 DataSync에 스토리지 보안 인증을 제공하세요.
    - 액세스 키에 클라우드 객체 스토리지에 액세스할 ID를 입력합니다.
    - 보안 키에 클라우드 개체 스토리지에 액세스할 암호를 입력합니다. 키를 직접 입력하거나 키가 포함된 AWS Secrets Manager 보안 암호를 지정할 수 있습니다. 자세한 내용은 스토리지 위치에 대한 자격 증명 제공을 참조하세요.
10. (선택 사항) 키와 값 필드에는 위치에 태그를 지정하기 위한 값을 입력합니다.

    태그는 AWS 리소스를 관리, 필터링 및 검색하는 데 도움이 됩니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.
11. 위치 생성을 선택합니다.

다음 단계

클라우드 객체 스토리지를 위한 DataSync 위치 생성을 완료한 후 전송 설정을 계속할 수 있습니다. 고려해야 할 몇 가지 단계는 다음과 같습니다.

1. 아직 만들지 않았다면 또다른 장소를 만들어서 AWS에서 데이터를 주고 받도록 계획합니다 .
2. DataSync가 객체 스토리지 위치의 메타데이터와 특수 파일을 처리하는 방법을 알아봅니다.
3. 데이터 전송 방식을 구성하세요. 예를 들어 데이터의 일부만 전송하길 원할 수 있습니다.

> **Important**
>
> DataSync가 객체 태그를 올바르게 복사하는 방법을 구성했는지 확인합니다. 자세한 내용은 객체 태그 사용의 고려 사항을 참조하세요.

4. 전송을 시작하세요.

사용자 데이터 전송을 위한 작업 생성

작업은가 데이터를 AWS DataSync 전송하는 위치와 방법을 설명합니다. 작업은 다음과 같이 구성됩니다.

- 소스 위치 - DataSync가 데이터를 전송하는 소스 스토리지 시스템 또는 서비스입니다.
- 대상 위치 - DataSync가 데이터를 전송하는 대상 스토리지 시스템 또는 서비스입니다.
- 작업 옵션 - 전송할 파일, 데이터 확인 방법, 작업 실행 시기 등의 설정입니다.
- 태스크 실행 - 태스크를 실행하는 것을 태스크 실행이라고 합니다.

작업 생성

DataSync 작업을 생성할 때 소스 및 대상 위치를 지정합니다. 전송할 파일, 메타데이터 처리 방법, 일정 설정 등을 선택하여 작업을 사용자 지정할 수도 있습니다.

작업을 생성하기 전에 DataSync 전송 방식을 이해하고 작업 할당량을 검토해야 합니다.

> **Important**
>
> Amazon S3 위치와 데이터를 주고받을 계획이라면 시작하기 전에 DataSync가 S3 요청 요금에 미치는 영향 및 DataSync 요금 페이지를 검토하세요.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 데이터를 전송 AWS 리전 하려는 중 하나에 있는지 확인합니다.
3. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
4. 소스 위치 구성 페이지에서 소스 위치를 생성하거나 선택하고 다음을 선택합니다.
5. 대상 위치 구성 페이지에서 대상 위치를 생성하거나 선택하고 다음을 선택합니다.
6. (권장) 설정 구성 페이지에서 작업에 기억할 수 있는 이름을 지정합니다.
7. 설정 구성 페이지에서 작업 옵션을 선택하거나 기본 설정을 사용합니다.

   다음 옵션 중 일부에 관심이 있을 수 있습니다.

   - 사용할 작업 모드를 지정합니다.
   - 매니페스트 또는 필터를 사용하여 전송할 데이터를 지정합니다.
   - 파일 메타데이터를 처리하고 데이터 무결성을 확인하는 방법을 구성합니다.
   - 작업 보고서 또는 Amazon CloudWatch를 사용하여 전송을 모니터링합니다. 작업에 대한 일종의 모니터링을 설정하는 것이 좋습니다.

   완료했으면 다음을 선택합니다.
8. 작업 구성을 검토한 후 작업 생성을 선택합니다.

작업을 시작할 준비가 되었습니다.

사용 AWS CLI

DataSync 소스 및 대상 위치를 생성하면 작업을 생성할 수 있습니다.

1. AWS CLI 설정에서 데이터를 전송 AWS 리전 하려는 중 하나를 사용하고 있는지 확인합니다.
2. 다음 `create-task`명령을 복사합니다.

```
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. `--source-location-arn`에서 소스 위치의 Amazon 리소스 이름(ARN)을 지정합니다.
4. `--destination-location-arn`에서 대상 위치의 ARN을 지정합니다.

   AWS 리전 또는 계정 간에 전송하는 경우 ARN에 다른 리전 또는 계정 ID가 포함되어 있는지 확인합니다.
5. (권장) `--name`에서 기억할 수 있는 작업의 이름을 지정합니다.
6. 필요에 따라 다른 작업 옵션을 지정합니다. 다음 옵션 중 일부에 관심이 있을 수 있습니다.

   - 매니페스트 또는 필터를 사용하여 전송할 데이터를 지정합니다.
   - 파일 메타데이터를 처리하고 데이터 무결성을 확인하는 방법을 구성합니다.
   - 작업 보고서 또는 Amazon CloudWatch를 사용하여 전송을 모니터링합니다. 작업에 대한 일종의 모니터링을 설정하는 것이 좋습니다.

   자세한 옵션은 create-task 섹션을 참조하세요. 다음은 여러 옵션을 지정하는 예제 `create-task` 명령입니다.

```
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. `create-task` 명령을 실행합니다.

   명령이 성공하면 생성한 작업의 ARN을 보여주는 응답을 받게 됩니다. 예제:

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

작업을 시작할 준비가 되었습니다.

태스크 상태

DataSync 작업을 생성할 때 상태를 확인하여 실행할 준비가 되었는지 확인할 수 있습니다.

콘솔 상태	API 상태	설명
Available	AVAILABLE	작업이 데이터 전송을 시작할 준비가 되었습니다.
실행	RUNNING	작업 실행이 진행 중입니다. 자세한 내용은 태스크 실행 상태 단원을 참조하십시오.
Unavailable	UNAVAILABLE	태스크에 사용되는 DataSync 에이전트는 오프라인 상태입니다. 자세한 내용은 에이전트가 오프라인 상태인 경우, 어떻게 해야 하나요? 섹션을 참조하세요.
대기됨	QUEUED	동일한 DataSync 에이전트를 사용하는 다른 작업 실행이 진행 중입니다. 자세한 내용은 작업이 대기열에 있는 시점 파악 단원을 참조하십시오.

여러 작업으로 대규모 데이터세트 파티셔닝

수백만 개의 파일 또는 객체 마이그레이션과 같은 대규모 데이터 세트를 전송하는 경우 전송에 DataSync Enhanced 모드를 사용하는 것이 좋습니다.이 모드는 거의 무제한의 파일로 데이터 세트를 전송할 수 있습니다. 수십억 개의 파일이 있는 매우 큰 데이터 세트의 경우 여러 DataSync 작업으로 데이터 세트를 분할하는 것을 고려해야 합니다. 여러 작업(및 위치에 따라 에이전트)에 데이터를 분할하면 DataSync가 데이터를 준비하고 전송하는 데 걸리는 시간을 줄일 수 있습니다.

여러 DataSync 작업에 걸쳐 대규모 데이터세트를 분할할 수 있는 몇 가지 방법을 고려하세요.

- 개별 폴더를 전송하는 작업을 생성합니다. 예를 들어 소스 스토리지에서 각각 `/FolderA` 및 `/FolderB`를 대상으로 하는 두 개의 작업을 생성할 수 있습니다.
- 매니페스트 또는 필터를 사용하여 파일, 객체, 폴더의 하위 집합을 전송하는 작업을 생성합니다.

이러한 접근 방식으로 스토리지 시스템의 I/O 작업이 증가하고 네트워크 대역폭에 영향을 미칠 수 있다는 점에 유의하세요. 자세한 내용은 How to accelerate your data transfers with DataSync scale out architectures에 관한 블로그를 참조하세요.

여러 작업을 사용하여 전송된 데이터 분할

서로 다른 데이터세트를 동일한 대상으로 전송하는 경우 전송하는 데이터를 분할하는 데 도움이 되는 여러 작업을 생성할 수 있습니다.

예를 들어 MyBucket이라는 동일한 S3 버킷으로 전송하는 경우 각 작업에 해당하는 다른 접두사를 버킷에 생성할수 있습니다. 이 접근 방식은 파일 이름이 데이터세트와 충돌하는 것을 방지하고 각 접두사에 대해 서로 다른 권한을 설정할 수 있습니다. 이를 설정하는 방법은 다음과 같습니다.

1. task1, task2, task3라는 이름의 대상 MyBucket에 세 개의 접두사를 생성합니다.
   - s3://MyBucket/task1
   - s3://MyBucket/task2
   - s3://MyBucket/task3
2. task1, task2, task3라는 이름의 DataSync 작업 세 개를 생성하여 MyBucket의 해당 접두사로 전송합니다.

데이터 전송을 위한 작업 모드 선택

AWS DataSync 작업은 다음 모드 중 하나로 실행할 수 있습니다.

- 향상된 모드 - 기본 모드보다 성능이 뛰어난 파일 또는 객체를 사실상 무제한으로 전송합니다. 확장 모드 작업은 데이터를 병렬로 나열, 준비, 전송, 확인하여 데이터 전송 프로세스를 최적화합니다. 향상된 모드는 현재 Amazon S3 위치 간 전송, 에이전트 없이 Azure Blob와 Amazon S3 간 전송, 에이전트 없이 다른 클라우드와 Amazon S3 간 전송, 향상된 모드 에이전트를 사용하여 NFS 또는 SMB 파일 서버와 Amazon S3 간 전송에 사용할 수 있습니다.
- 기본 모드 - AWS 스토리지와 지원되는 다른 모든 DataSync 위치 간에 파일 또는 객체를 전송합니다. 기본 모드 작업에는 데이터세트의 파일, 객체, 디렉터리 수에 대한 할당량이 적용됩니다. 기본 모드는 데이터를 순차적으로 준비, 전송, 확인하므로 대부분의 워크로드에서 확장 모드보다 느립니다.

작업 모드 차이점 이해

다음 정보는 사용할 작업 모드를 결정하는 데 도움이 될 수 있습니다.

기능	확장 모드 동작	기본 모드 동작
성능	DataSync는 데이터를 병렬로 나열, 준비, 전송, 확인합니다. 대부분의 워크로드에 대해 기본 모드보다 높은 성능 제공(대용량 객체 전송 등)	DataSync는 데이터를 순차적으로 준비, 전송, 확인합니다. 대부분의 워크로드에서 확장 모드보다 성능이 느림
DataSync가 작업 실행당 사용할 수 있는 데이터세트의 항목 수	사실상 무제한의 객체	할당량 적용
데이터 전송 카운터 및 지표	DataSync가 소스 위치에서 찾는 객체 수, 각 작업 실행 중에 준비되는 객체 수, 파일 및 객체 카운터와 유사한 폴더 카운터 등 기본 모드보다 더 많은 카운터 및 지표	확장 모드보다 카운터 및 지표가 적음
로깅	정형 로그(JSON 형식)	비정형 로그
지원 위치	현재 Amazon S3 위치 간 전송, 에이전트 없이 Azure Blob와 Amazon S3 간 전송, 에이전트 없이 다른 클라우드와 Amazon S3 간 전송, 향상된 모드 에이전트를 사용하여 NFS 또는 SMB 파일 서버와 Amazon S3 간 전송의 경우.	DataSync가 지원하는 모든 위치 간 전송의 경우
데이터 확인 옵션	DataSync가 전송된 데이터만 확인	DataSync가 기본적으로 모든 데이터를 확인
비용	자세한 내용은 DataSync 요금 페이지를 참조하세요.	자세한 내용은 DataSync 요금 페이지를 참조하세요.
지원하지 않는 객체 태그에 대한 장애 처리	객체 태그 지정을 지원하지 않는 위치로 클라우드 스토리지	객체 태그 지정을 지원하지 않는 위치로 클라우드 스토리

기능	확장 모드 동작	기본 모드 동작
	를 전송하거나 해당 위치에서 전송 받는 경우 `ObjectTags` 옵션이 지정되지 않거나 `PRESERVE`으로 설정되어 있으면 작업 실행이 즉시 실패합니다.	지를 전송하거나 해당 위치에서 전송 받는 경우 작업 실행이 정상적으로 수행되지만 `ObjectTags` 옵션이 지정되지 않았거나 `PRESERVE`로 설정되어 있으면 태그가 지정된 객체에 대한 객체별 실패를 보고합니다.

작업 모드 선택

향상된 모드 에이전트를 사용하여 Amazon S3 위치 간 전송, 에이전트 없이 Azure Blob와 Amazon S3 간 전송, 에이전트 없이 다른 클라우드와 Amazon S3 간 전송, NFS 또는 SMB 파일 서버와 Amazon S3 간 전송에 대해서만 향상된 모드를 선택할 수 있습니다. 그렇지 않으면 기본 모드를 사용해야 합니다. 예를 들어 온프레미스 HDFS 위치에서 S3 위치로 전송하려면 기본 모드가 필요합니다.

작업 옵션과 성능은 선택한 작업 모드에 따라 다를 수 있습니다. 작업을 생성한 후에는 작업 모드를 변경할 수 없습니다.

필수 권한

확장 모드 작업을 생성하려면 DataSync를 사용하는 IAM 역할에 `iam:CreateServiceLinkedRole` 권한이 있어야 합니다.

DataSync 사용자 권한을 설정하려면 AWSDataSyncFullAccess를 사용하는 것이 좋습니다. 이는 사용자에게 DataSync에 대한 전체 액세스 권한과 해당 종속성에 대한 최소 액세스를 제공하는 AWS 관리형 정책입니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 작업 모드의 경우, 다음 옵션 중 하나를 선택합니다.

- Enhanced
- 기본

자세한 내용은 작업 모드 차이점 이해 단원을 참조하십시오.

5. 설정 구성 페이지에서 작업 옵션을 선택하거나 기본 설정을 사용합니다.

   다음 옵션 중 일부에 관심이 있을 수 있습니다.

   - 매니페스트 또는 필터를 사용하여 전송할 데이터를 지정합니다.
   - 파일 메타데이터를 처리하고 데이터 무결성을 확인하는 방법을 구성합니다.
   - 작업 보고서 또는 Amazon CloudWatch Logs를 사용하여 전송을 모니터링합니다.

   완료했으면 다음을 선택합니다.

6. 작업 구성을 검토한 후 작업 생성을 선택합니다.

사용 AWS CLI

1. AWS CLI 설정에서 데이터를 전송 AWS 리전 하려는 중 하나를 사용하고 있는지 확인합니다.
2. 다음 `create-task`명령을 복사합니다.

```
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. `--source-location-arn`에서 소스 위치의 Amazon 리소스 이름(ARN)을 지정합니다.
4. `--destination-location-arn`에서 대상 위치의 ARN을 지정합니다.

   AWS 리전 또는 계정 간에 전송하는 경우 ARN에 다른 리전 또는 계정 ID가 포함되어 있는지 확인합니다.

5. `--task-mode`에 대해 `ENHANCED` 또는 `BASIC`을 지정합니다.

   자세한 내용은 작업 모드 차이점 이해 단원을 참조하십시오.

6. 필요에 따라 다른 작업 옵션을 지정합니다. 다음 옵션 중 일부에 관심이 있을 수 있습니다.

- 매니페스트 또는 필터를 사용하여 전송할 데이터를 지정합니다.
- 파일 메타데이터를 처리하고 데이터 무결성을 확인하는 방법을 구성합니다.
- 작업 보고서 또는 Amazon CloudWatch Logs를 사용하여 전송을 모니터링합니다.

자세한 옵션은 create-task 섹션을 참조하세요. 다음은 확장 모드 및 여러 기타 옵션을 지정하는 `create-task` 명령의 예시입니다.

```
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. `create-task` 명령을 실행합니다.

   명령이 성공하면 생성한 작업의 ARN을 보여주는 응답을 받게 됩니다. 예제:

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

DataSync API 사용

CreateTask 작업에서 `TaskMode` 파라미터를 구성하여 DataSync 작업 모드를 지정할 수 있습니다.

AWS DataSync 전송할 항목 선택

AWS DataSync 를 사용하면 전송할 항목과 데이터 처리 방법을 선택할 수 있습니다. 몇 가지 옵션은 다음과 같습니다.

- 매니페스트를 사용하여 파일 또는 객체의 정확한 목록을 전송합니다.
- 필터를 사용하여 전송에 특정 유형의 데이터를 포함하거나 제외합니다.
- 반복 전송의 경우 마지막 전송 이후 변경된 데이터만 이동합니다.

- 소스 위치에 있는 것과 일치하도록 대상 위치의 데이터를 덮어씁니다.
- 스토리지 위치 간에 보존할 파일 또는 객체 메타데이터를 선택합니다.

주제

- 매니페스트를 사용하여 특정 파일 또는 객체 전송
- 필터를 사용하여 특정 파일, 객체 및 폴더 전송
- DataSync가 파일 및 객체 메타데이터를 처리하는 방법 이해
- 에서 복사한 링크 및 디렉터리 AWS DataSync
- 파일, 객체 및 메타데이터 처리 방법 구성

매니페스트를 사용하여 특정 파일 또는 객체 전송

매니페스트는 전송 AWS DataSync 하려는 파일 또는 객체의 목록입니다. 예를 들어 잠재적으로 수백만 개의 객체가 있는 S3 버킷의 모든 것을 전송해야 하는 대신 DataSync는 매니페스트에 나열한 객체만 전송합니다.

매니페스트는 필터와 비슷하지만 필터 패턴과 일치하는 데이터 대신 전송할 파일 또는 객체를 정확하게 식별할 수 있습니다.

> **Note**
>
> 확장 모드 작업을 포함한 매니페스트 파일의 최대 허용 크기는 20GB입니다.

매니페스트 생성

매니페스트는 DataSync가 전송할 소스 위치의 파일 또는 객체를 나열하는 쉼표로 구분된 값(CSV) 형식의 파일입니다. 소스가 S3 버킷인 경우 전송할 객체 버전을 포함할 수도 있습니다.

주제

- 지침
- 매니페스트 예제

지침

이 지침을 사용하면 DataSync에서 작동하는 매니페스트를 생성하는 데 도움이 됩니다.

Do

- 전송하려는 각 파일 또는 객체의 전체 경로를 지정합니다.

  모든 콘텐츠를 전송할 의도로 디렉터리 또는 폴더만 지정할 수는 없습니다. 이러한 상황에서는 매니페스트 대신 포함 필터를 사용하는 것이 좋습니다.
- 각 파일 또는 객체 경로가 DataSync 소스 위치를 구성할 때 지정한 마운트 경로, 폴더, 디렉터리 또는 접두사와 관련이 있는지 확인합니다.

  예를 들어 접두사가 `photos`인 S3 위치를 구성한다고 가정해 보겠습니다. 이 접두사에는 전송하려는 `my-picture.png` 객체가 포함됩니다. 매니페스트에서 접두사 및 객체(`photos/my-picture.png`) 대신 객체(`my-picture.png`)만 지정하면 됩니다.
- Amazon S3 객체 버전 ID를 지정하려면 쉼표를 사용하여 객체의 경로와 버전 ID를 구분합니다.

  다음 예제에서는 두 개의 필드가 있는 매니페스트 항목을 보여줍니다. 첫 번째 필드에는 `picture1.png`라는 객체가 포함됩니다. 두 번째 필드는 쉼표로 구분되며 `111111`의 버전 ID를 포함합니다.

  ```
  picture1.png,111111
  ```
- 다음과 같은 상황에서는 따옴표를 사용합니다.
  - 경로에 특수 문자(쉼표, 따옴표, 줄 끝)가 포함된 경우:

    ```
    "filename,with,commas.txt"
    ```
  - 경로가 여러 줄에 걸쳐 있는 경우:

    ```
    "this
    is
    a
    filename.txt"
    ```
  - 경로에 따옴표가 포함된 경우:

    ```
    filename""with""quotes.txt
    ```

    이는 `filename"with"quotes.txt`라는 경로를 나타냅니다.

  이러한 따옴표 규칙은 버전 ID 필드에도 적용됩니다. 일반적으로 매니페스트 필드에 따옴표가 있는 경우 다른 따옴표로 이스케이프해야 합니다.
- 각 파일 또는 객체 항목을 새 줄로 구분합니다.

Linux(라인 피드 또는 캐리지 반환) 또는 Windows(캐리지 반환 후 라인 피드) 스타일 라인 분리를 사용하여 라인을 분리할 수 있습니다.

- 매니페스트(예: `my-manifest.csv` 또는 `my-manifest.txt`)를 저장합니다.
- DataSync가 액세스할 수 있는 S3 버킷에 매니페스트를 업로드합니다.

  이 버킷은 DataSync를 사용하는 동일한 AWS 리전 또는 계정에 있을 필요는 없습니다.

Don't

- 모든 콘텐츠를 전송할 의도로 디렉터리 또는 폴더만 지정합니다.

  매니페스트는 전송하려는 파일 또는 객체에 대한 전체 경로만 포함할 수 있습니다. 특정 탑재 경로, 폴더, 디렉터리 또는 접두사를 사용하도록 소스 위치를 구성하는 경우 매니페스트에 포함할 필요가 없습니다.
- 4,096자를 초과하는 파일 또는 객체 경로를 지정합니다.
- 1,024바이트를 초과하는 파일 경로, 객체 경로 또는 Amazon S3 객체 버전 ID를 지정합니다.
- 중복 파일 또는 객체 경로를 지정합니다.
- 소스 위치가 S3 버킷이 아닌 경우 객체 버전 ID를 포함합니다.
- 매니페스트 항목에 두 개 이상의 필드를 포함합니다.

  항목에는 파일 또는 객체 경로와 (해당하는 경우) Amazon S3 객체 버전 ID만 포함될 수 있습니다.
- UTF-8 인코딩을 준수하지 않는 문자를 포함합니다.
- 따옴표 외부의 입력 필드에 의도하지 않은 공백을 포함합니다.

매니페스트 예제

이 예제를 사용하면 DataSync에서 작동하는 매니페스트를 생성하는 데 도움이 됩니다.

전체 파일 또는 객체 경로가 있는 매니페스트

다음 예제에서는 전송할 전체 파일 또는 객체 경로가 있는 매니페스트를 보여줍니다.

```
photos/picture1.png
photos/picture2.png
photos/picture3.png
```

객체 키만 있는 매니페스트

다음 예제에서는 Amazon S3 소스 위치에서 전송할 객체가 있는 매니페스트를 보여줍니다. 위치는 접두사 photos로 구성되므로 객체 키만 지정됩니다.

```
picture1.png
picture2.png
picture3.png
```

객체 경로 및 버전 ID가 있는 매니페스트

다음 매니페스트 예제의 처음 두 항목에는 전송할 특정 Amazon S3 객체 버전이 포함됩니다.

```
photos/picture1.png,111111
photos/picture2.png,121212
photos/picture3.png
```

UTF-8 문자가 포함된 매니페스트

다음 예제에서는 UTF-8 문자가 포함된 파일이 있는 매니페스트를 보여줍니다.

```
documents/résumé1.pdf
documents/résumé2.pdf
documents/résumé3.pdf
```

DataSync에 매니페스트 액세스 권한 제공

DataSync에 S3 버킷의 매니페스트에 대한 액세스 권한을 부여하는 AWS Identity and Access Management (IAM) 역할이 필요합니다. 이 역할에는 다음 권한이 포함되어야 합니다.

- `s3:GetObject`
- `s3:GetObjectVersion`

DataSync 콘솔에서 이 역할을 자동으로 생성하거나 직접 생성할 수 있습니다.

> **Note**
>
> 매니페스트가 다른에 AWS 계정있는 경우이 역할을 수동으로 생성해야 합니다.

IAM 역할 자동 생성

콘솔에서 전송 작업을 생성하거나 시작할 때 DataSync는 매니페스트에 액세스하는 데 필요한 `s3:GetObject` 및 `s3:GetObjectVersion` 권한을 사용하여 IAM 역할을 생성할 수 있습니다.

역할을 자동으로 생성하기 위해 필요한 권한

역할을 자동으로 생성하려면 DataSync 콘솔에 액세스하는 데 사용하는 역할에 다음 권한이 있는지 확인합니다.

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:AttachRolePolicy`

IAM 역할 생성(동일한 계정)

DataSync가 매니페스트에 액세스하는 데 필요한 IAM 역할을 수동으로 생성할 수 있습니다. 다음 지침은 DataSync를 사용하고 매니페스트의 S3 버킷이 있는 동일한 AWS 계정 에 있다고 가정합니다.

1. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
2. 왼쪽 탐색 창의 액세스 관리에서 역할을 선택한 다음, 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택 페이지에서 신뢰할 수 있는 엔터티 유형으로 AWS 서비스를 선택합니다.
4. 사용 사례로 드롭다운 목록에서 DataSync를 선택하고 DataSync를 선택합니다. 다음을 선택합니다.
5. 권한 추가 페이지에서 다음을 선택합니다. 역할 이름을 제공하고 역할 생성을 선택합니다.
6. 역할 페이지에서 방금 생성한 역할의 이름을 검색해 선택합니다.
7. 역할의 세부 정보 페이지에서 권한 탭을 선택합니다. 권한 추가를 선택한 후 인라인 정책 추가를 선택합니다.
8. JSON 탭을 선택하고 다음 샘플 정책을 정책 편집기에 붙여 넣습니다.

   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. 방금 붙여넣은 샘플 정책에서 다음 값을 자체 값으로 바꿉니다.

   a. *amzn-s3-demo-bucket*을 매니페스트를 호스팅하는 S3 버킷의 이름으로 바꿉니다.

   b. *my-manifest.csv*를 매니페스트 파일의 이름으로 바꿉니다.

10. 다음을 선택합니다. 정책에 이름을 제공하고 정책 생성을 선택합니다.

11. (권장) 교차 서비스 혼동된 대리자 문제를 방지하려면 다음을 수행합니다.

    a. 역할의 세부 정도 페이지에서 신뢰 관계 탭을 선택합니다. 신뢰 정책 편집을 선택합니다.

    b. `aws:SourceArn` 및 `aws:SourceAccount`전역 조건 컨텍스트 키가 포함된 다음 예를 사용하여 신뢰 정책을 업데이트하세요.

    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:*"
            }
        }
      }
  ]
```

```
}
```

- 각 인스턴스를 DataSync를 사용하는 AWS 계정 ID*account-id*로 바꿉니다.
- 를 DataSync를 사용하는 AWS 리전 *region*로 바꿉니다.

c. 정책 업데이트를 선택합니다.

DataSync가 매니페스트에 액세스하도록 허용하는 IAM 역할을 생성했습니다. 작업을 생성하거나 시작할 때 이 역할을 지정합니다.

IAM 역할 생성(다른 계정)

매니페스트가 다른에 속하는 S3 버킷에 있는 AWS 계정경우 DataSync가 매니페스트에 액세스하는 데 사용하는 IAM 역할을 수동으로 생성해야 합니다. 그런 다음 매니페스트가 AWS 계정 있는에서 S3 버킷 정책에 역할을 포함해야 합니다.

역할 만들기

1. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
2. 왼쪽 탐색 창의 액세스 관리에서 역할을 선택한 다음, 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택 페이지에서 신뢰할 수 있는 엔터티 유형으로 AWS 서비스를 선택합니다.
4. 사용 사례로 드롭다운 목록에서 DataSync를 선택하고 DataSync를 선택합니다. 다음을 선택합니다.
5. 권한 추가 페이지에서 다음을 선택합니다. 역할 이름을 제공하고 역할 생성을 선택합니다.
6. 역할 페이지에서 방금 생성한 역할의 이름을 검색해 선택합니다.
7. 역할의 세부 정보 페이지에서 권한 탭을 선택합니다. 권한 추가를 선택한 후 인라인 정책 추가를 선택합니다.
8. JSON 탭을 선택하고 다음 샘플 정책을 정책 편집기에 붙여 넣습니다.

   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. 방금 붙여넣은 샘플 정책에서 다음 값을 자체 값으로 바꿉니다.

   a. *amzn-s3-demo-bucket*을 매니페스트를 호스팅하는 S3 버킷의 이름으로 바꿉니다.

   b. *my-manifest.csv*를 매니페스트 파일의 이름으로 바꿉니다.

10. 다음을 선택합니다. 정책에 이름을 제공하고 정책 생성을 선택합니다.

11. (권장) 교차 서비스 혼동된 대리자 문제를 방지하려면 다음을 수행합니다.

    a. 역할의 세부 정도 페이지에서 신뢰 관계 탭을 선택합니다. 신뢰 정책 편집을 선택합니다.

    b. `aws:SourceArn` 및 `aws:SourceAccount`전역 조건 컨텍스트 키가 포함된 다음 예를 사용하여 신뢰 정책을 업데이트하세요.

    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:*"
            }
        }
     }
  ]
```

```
}
```

- 의 각 인스턴스를 DataSync를 사용하는 AWS 계정 ID*account-id*로 바꿉니다.
- 를 DataSync를 사용하는 AWS 리전 *region*로 바꿉니다.

c. 정책 업데이트를 선택합니다.

S3 버킷 정책에 포함할 수 있는 IAM 역할을 생성했습니다.

역할로 S3 버킷 정책 업데이트

IAM 역할을 생성한 후에는 매니페스트가 AWS 계정 있는 다른의 S3 버킷 정책에 추가해야 합니다.

1. 에서 매니페스트의 S3 버킷이 있는 계정으로 AWS Management Console전환합니다.
2. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
3. 버킷 세부 사항 페이지에서 권한 탭을 선택합니다.
4. 버킷 정책에서 편집을 선택하고 다음을 수행하여 S3 버킷 정책을 수정하세요.

   a. 편집기에 있는 내용을 업데이트하여 다음 정책 설명을 포함하세요.

      JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncAccessManifestBucket",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

   b. 를 DataSync를 사용하는 계정의 AWS 계정 ID로 *account-id* 바꿉니다.

c. *datasync-role*을 방금 생성한 IAM 역할로 바꾸면 DataSync가 매니페스트에 액세스할 수 있습니다.

d. *amzn-s3-demo-bucket*을 다른 AWS 계정에서 매니페스트를 호스팅하는 S3 버킷의 이름으로 바꿉니다.

5. 변경 사항 저장을 선택합니다.

DataSync가 다른 계정의 매니페스트에 액세스하도록 허용하는 IAM 역할을 생성했습니다. 작업을 생성하거나 시작할 때 이 역할을 지정합니다.

작업 생성 시 매니페스트 지정

작업을 생성할 때 DataSync가 사용할 매니페스트를 지정할 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 작업을 선택한 후 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 스캔할 콘텐츠에서 특정 파일, 객체 및 폴더를 선택한 다음 매니페스트 사용을 선택합니다.
5. S3 URI에서 S3 버킷에 호스팅되는 매니페스트를 선택합니다.

   또는 URI(예: `s3://bucket/prefix/my-manifest.csv`)를 입력할 수 있습니다.
6. 객체 버전에서 DataSync가 사용할 매니페스트의 버전을 선택합니다.

   기본적으로 DataSync는 최신 버전의 객체를 사용합니다.
7. 매니페스트 액세스 역할에서 다음 중 하나를 수행합니다.

   - DataSync가 S3 버킷의 매니페스트에 액세스하는 데 필요한 권한을 가진 IAM 역할을 자동으로 생성하도록 자동 생성을 선택합니다.
   - 매니페스트에 액세스할 수 있는 기존 IAM 역할을 선택합니다.

   자세한 내용은 DataSync에 매니페스트 액세스 권한 제공 단원을 참조하십시오.
8. 필요한 다른 작업 설정을 구성한 후 다음을 선택합니다.
9. 작업 생성을 선택합니다.

사용 AWS CLI

1. 다음 `create-task`명령을 복사합니다.

```
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. `--source-location-arn` 파라미터에서 데이터를 전송하는 소스 위치의 Amazon 리소스 이름(ARN)을 지정합니다.
3. `--destination-location-arn` 파라미터에서 데이터를 전송하는 대상 위치의 ARN을 지정합니다.
4. `--manifest-config` 파라미터에 관하여 다음을 수행합니다.

   - `ManifestObjectPath`-매니페스트의 S3 객체 키를 지정합니다.
   - `BucketAccessRoleArn`-DataSync가 S3 버킷의 매니페스트에 액세스하도록 허용하는 IAM 역할을 지정합니다.

     자세한 내용은 DataSync에 매니페스트 액세스 권한 제공 단원을 참조하십시오.

   - `S3BucketArn`-매니페스트를 호스팅하는 S3 버킷의 ARN을 지정합니다.
   - `ManifestObjectVersionId`-DataSync에서 사용할 매니페스트의 버전을 지정합니다.

     기본적으로 DataSync는 최신 버전의 객체를 사용합니다.
5. `create-task` 명령을 실행하여 작업을 생성합니다.

준비가 되면 전송 작업을 시작할 수 있습니다.

작업을 시작할 때 매니페스트 지정

작업을 실행할 때 DataSync가 사용할 매니페스트를 지정할 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 작업을 선택한 다음 시작할 작업을 선택합니다.
3. 작업 개요 페이지에서 시작을 선택한 다음 재정의 옵션으로 시작을 선택합니다.
4. 스캔할 콘텐츠에서 특정 파일, 객체 및 폴더를 선택한 다음 매니페스트 사용을 선택합니다.
5. S3 URI에서 S3 버킷에 호스팅되는 매니페스트를 선택합니다.

   또는 URI(예: `s3://bucket/prefix/my-manifest.csv`)를 입력할 수 있습니다.
6. 객체 버전에서 DataSync가 사용할 매니페스트의 버전을 선택합니다.

   기본적으로 DataSync는 최신 버전의 객체를 사용합니다.
7. 매니페스트 액세스 역할에서 다음 중 하나를 수행합니다.

   - DataSync에 대해 자동 생성을 선택하여 S3 버킷에서 매니페스트에 액세스할 IAM 역할을 자동으로 생성합니다.
   - 매니페스트에 액세스할 수 있는 기존 IAM 역할을 선택합니다.

   자세한 내용은 DataSync에 매니페스트 액세스 권한 제공 단원을 참조하십시오.
8. 시작을 선택하여 전송을 시작합니다.

사용 AWS CLI

1. 다음 `start-task-execution`명령을 복사합니다.

```
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. `--task-arn` 파라미터에는 시작하려는 작업의 Amazon 리소스 이름(ARN)을 지정합니다.
3. `--manifest-config` 파라미터에 관하여 다음을 수행합니다.

   - `ManifestObjectPath`-매니페스트의 S3 객체 키를 지정합니다.
   - `BucketAccessRoleArn`-DataSync가 S3 버킷의 매니페스트에 액세스하도록 허용하는 IAM 역할을 지정합니다.

     자세한 내용은 DataSync에 매니페스트 액세스 권한 제공 단원을 참조하십시오.

   - `S3BucketArn`-매니페스트를 호스팅하는 S3 버킷의 ARN을 지정합니다.
   - `ManifestObjectVersionId`-DataSync에서 사용할 매니페스트의 버전을 지정합니다.

     기본적으로 DataSync는 최신 버전의 객체를 사용합니다.
4. `start-task-execution` 명령을 실행하여 전송을 시작합니다.

제한 사항

- 매니페스트를 필터와 함께 사용할 수 없습니다.
- 모든 콘텐츠를 전송할 의도로 디렉터리 또는 폴더만 지정할 수는 없습니다. 이러한 상황에서는 매니페스트 대신 포함 필터를 사용하는 것이 좋습니다.
- 삭제된 파일 유지 작업 옵션(API의 `PreserveDeletedFiles`)을 사용하여 소스에 없는 대상의 파일 또는 객체를 유지할 수 없습니다. DataSync는 매니페스트에 나열된 항목만 전송하며 대상의 아무것도 삭제하지 않습니다.

문제 해결

`HeadObject` 또는 `GetObjectTagging` 관련 오류

S3 버킷에서 특정 버전 ID가 있는 객체를 전송하는 경우 `HeadObject` 또는 `GetObjectTagging` 관련 오류가 발생할 수 있습니다. 예를 들어 `GetObjectTagging` 관련 오류는 다음과 같습니다.

```
[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
```

이러한 오류 중 하나가 표시되면 DataSync가 S3 소스 위치에 액세스하는 데 사용하는 IAM 역할에 다음 권한이 있는지 확인합니다.

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

이러한 권한으로 역할을 업데이트해야 하는 경우 DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성 섹션을 참조하세요.

오류: **`ManifestFileDoesNotExist`**

이 오류는 매니페스트 내의 파일을 소스에서 찾을 수 없음을 나타냅니다. 매니페스트 생성 지침을 검토합니다.

다음 단계

아직 작업을 시작하지 않은 경우 작업을 시작합니다. 그렇지 않으면 작업의 활동을 모니터링합니다.

필터를 사용하여 특정 파일, 객체 및 폴더 전송

AWS DataSync 를 사용하면 필터를 적용하여 전송 시 소스 위치에서 데이터를 포함하거나 제외할 수 있습니다. 예를 들어 `.tmp`로 끝나는 임시 파일을 전송하지 않으려면 해당 파일이 대상 위치로 전송되지 않게 하는 제외 필터를 생성할 수 있습니다.

동일한 전송 작업에 제외 필터와 포함 필터를 조합하여 사용할 수 있습니다. 작업의 필터를 수정하면 다음 번에 작업을 실행할 때 이러한 변경 사항이 적용됩니다.

필터링 용어, 정의 및 구문

DataSync 필터링과 관련된 개념을 숙지하세요.

필터

특정 필터(예, `*.tmp|*.temp`혹은 `/folderA|/folderB`)를 구성하는 전체 문자열입니다.

필터는 하나의 파이프(|)를 사용하여 구분되는 패턴으로 구성됩니다. 각 패턴을 개별적으로 추가하므로 DataSync 콘솔에 패턴을 추가할 때 구분 기호를 사용할 필요가 없습니다.

> **Note**
>
> 필터 값은 대소문자를 구분합니다. 예를 들어 필터 `/folderA`은 `/FolderA`와 일치하지 않습니다.

패턴

필터 내 패턴입니다. 예를 들어, `*.tmp`은 `*.tmp|*.temp`필터의 일부인 패턴입니다. 필터에 여러 패턴이 있는 경우 파이프(|)를 사용하여 각 패턴을 구분합니다.

폴더

- 모든 필터는 소스 위치 경로와 관련이 있습니다. 예를 들어, 사용자가 사용자 소스 위치와 작업을 생성할 때 `/my_source/`을 소스 경로로 지정한다면 포함 필터 `/transfer_this/`를 지정합니다. 이 경우 DataSync는 디렉터리 `/my_source/transfer_this/`과 그 콘텐츠만 전송합니다.
- 소스 위치 바로 밑에 직접 폴더를 지정하려면 폴더 이름 앞에 슬래시(/)를 포함시키십시오. 이전 예제에서 패턴은 `transfer_this`가 아닌 `/transfer_this`를 사용합니다.
- DataSync는 다음 패턴을 동일한 방식으로 해석하여 폴더와 해당 콘텐츠 모두를 일치시킵니다.

  `/dir`

  `/dir/`
- /Amazon S3 버킷로 혹은 거기에서 데이터를 전송할 때 DataSync는 객체 키의 문자를 파일 시스템의 폴더와 동등하게 취급합니다.

특수 문자

필터링에 사용할 특수 문자는 다음과 같습니다.

특수 문자	설명
*(와일드카드)	0개 이상의 문자를 일치시키는 데 사용되는 문자입니다. 예를 들어, `/movies_folder*` 는 `/movies_folder` 및 `/movies_folder1` 모두와 일치합니다.
|(파이프 구분 기호)	패턴 간 구분 기호로 사용되는 문자입니다. 이 문자를 사용하면 각각 필터와 일치하는 여러 패턴을 지정할 수 있습니다. 예를

특수 문자	설명
	들어, `*.tmp|*.temp`는 `tmp` 또는 `temp`로 끝나는 파일과 일치합니다. **Note** 각 패턴을 개별 행에 추가하므로 콘솔에 패턴을 추가할 때 이 구분 기호는 필요하지 않습니다.
\(백슬래시)	파일이나 객체 이름에 특수 문자(*, |, \)를 사용하지 마십시오. 백슬래시가 파일 이름의 일부인 경우 이중 백슬래시(\\)가 필요합니다. 마찬가지로, \\\\는 파일 이름에 두 개의 연속된 백슬래시가 있음을 나타냅니다. 파이프가 파일 이름의 일부인 경우 백슬래시 뒤 파이프(|)가 필요합니다. (\) 뒤에 다른 문자가 있거나 패턴 끝에 백 슬래시가 있으면 무시됩니다.

필터 예제

다음 예제에서는 DataSync에 사용할 수 있는 공통 필터를 보여 줍니다.

Note

필터에 사용할 수 있는 문자 수에는 제한이 있습니다. 자세한 설명은 DataSync 할당량섹션을 참조하세요.

소스 위치에서 일부 폴더 제외

경우에 따라 소스 위치의 폴더가 대상 위치로 복사 되지 않도록 제외 필터를 원할 수도 있습니다. 예를 들어, 작업 진행 중인 임시 폴더가 있는 경우 다음 필터와 같은 것을 사용할 수 있습니다.

```
*/.temp
```

비슷한 콘텐츠(예: /reports2021및/reports2022)) 가 있는 폴더를 제외하려면 다음과 같은 제외 필터를 사용할 수 있습니다.

```
/reports*
```

파일 계층 구조의 모든 레벨 폴더를 제외하려면 제외 필터를 다음과 같이 사용하면 됩니다.

```
*/folder-to-exclude-1|*/folder-to-exclude-2
```

소스 위치의 최상위 레벨 폴더를 제외하려면 제외 필터를 다음과 같이 사용하면 됩니다.

```
/top-level-folder-to-exclude-1|/top-level-folder-to-exclude-2
```

소스 위치에 폴더 서브셋을 포함시킵니다

경우에 따라 소스 위치가 대규모 공유가 되면 해당 루트 아래에 있는 폴더의 서브셋만 전송해야 합니다. 특정 폴더를 포함하려면 다음과 같은 포함 필터가 있는 작업 실행을 시작합니다.

```
/folder-to-transfer/*
```

특정 파일 유형 제외

전송에서 특정 파일 유형을 제외하려면 *.temp와 같은 제외 필터가 있는 작업 실행을 생성하면 됩니다.

지정한 개별 파일만 전송

일련의 개별 파일을 전송하려면 다음의 제외 필터가 있는 작업 실행을 시작합니다: “/folder/subfolder/file1.txt|/folder/subfolder/file2.txt|/folder/subfolder/file2.txt”

포함 필터 생성

포함 필터는 DataSync가 전송할 파일, 객체, 폴더를 정의합니다. 작업을 생성하거나 편집 또는 시작할 때 포함 필터를 구성할 수 있습니다.

DataSync는 포함 필터와 일치하는 파일 및 폴더만 스캔하고 전송합니다. 예를 들어, 소스 폴더의 서브셋만 포함하려면 /important_folder_1|/important_folder_2를 지정하면 됩니다.

> **Note**
>
> 포함 필터는 와일드 카드 (*) 문자를 패턴에서 오른쪽 끝에 둡니다. 예를 들어, /documents*|/code*는 지원되지만 *.txt은 지원되지 않습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 작업을 선택한 후 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 스캔할 콘텐츠에서 특정 파일, 객체 및 폴더를 선택한 다음 필터 사용을 선택합니다.
5. 포함에서 필터를 입력한 다음(예: 중요한 디렉터리를 포함하려면 `/important_folders`) 패턴 추가를 선택합니다.
6. 필요에 따라 다른 포함 필터를 추가합니다.

사용 AWS CLI

를 사용할 때는 필터 주위에 작은따옴표(')를 사용하고 필터가 두 개 이상인 경우 |(파이프)를 구분 기호로 사용해야 AWS CLI합니다.

다음 예제에서는 `create-task` 명령을 실행할 때 포함 필터 `/important_folder1`과 `/important_folder2` 두 가지를 지정합니다.

```
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'
```

제외 필터 생성

제외 필터는 DataSync가 전송하지 않도록 소스 위치의 파일, 객체 및 폴더를 정의합니다. 작업을 생성하거나 편집 또는 시작할 때 이러한 필터를 구성할 수 있습니다.

주제

- 기본값으로 제외된 데이터

기본값으로 제외된 데이터

DataSync는 일부 데이터가 전송되지 않도록 자동으로 제외합니다.

- `.snapshot`-DataSync는 `.snapshot`로 끝나는 모든 경로를 무시합니다. 이 경로는 일반적으로 스토리지 시스템의 파일 또는 디렉터리의 특정 시점 스냅샷에 사용됩니다.
- `/.aws-datasync` 및 `/.awssync`-DataSync는 전송을 용이하게 하기 위해 사용자 위치에 이러한 폴더를 생성합니다.
- `/.zfs`-Amazon FSx for OpenZFS의 위치에 이 폴더가 표시될 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 작업을 선택한 후 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 제외에서 필터를 입력한 다음(예: 임시 폴더를 제외하려면 `*/temp`) 패턴 추가를 선택합니다.
5. 필요에 따라 다른 제외 필터를 추가합니다.
6. 필요한 경우 포함 필터를 추가합니다.

사용 AWS CLI

를 사용할 때는 필터 주위에 작은따옴표(')를 사용하고 필터가 두 개 이상인 경우 |(파이프)를 구분 기호로 사용해야 AWS CLI합니다.

다음 예제에서는 `create-task` 명령을 실행할 때 제외 필터 `*/temp`과 `*/tmp` 두 가지를 지정합니다.

```
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'
```

DataSync가 파일 및 객체 메타데이터를 처리하는 방법 이해

AWS DataSync 는 데이터 전송 중에 파일 또는 객체 메타데이터를 보존할 수 있습니다. 메타데이터를 복사하는 방법은 전송 위치 및 전송 위치에서 유사한 유형의 메타데이터를 사용하는지 여부에 따라 달라집니다.

시스템 수준 메타데이터

일반적으로 DataSync는 시스템 수준 메타데이터를 복사하지 않습니다. 예를 들어, SMB 파일 서버에서 전송하는 경우, 파일 시스템 수준에서 구성한 권한은 목적지 스토리지 시스템에 복사되지 않습니다.

예외는 있습니다. Amazon S3와 다른 객체 스토리지 간에 전송할 때 DataSync는 일부시스템 정의 객체 메타데이터를 복사합니다.

Amazon S3 전송에서 복사된 메타데이터

다음 표는 전송에 Amazon S3 위치가 포함된 경우 DataSync가 복사할 수 있는 메타데이터를 설명합니다.

주제

- Amazon S3로
- Amazon S3와 다른 객체 스토리지 사이에서
- Amazon S3와 HDFS 사이에서

Amazon S3로

다음 위치 중 하나에서 복사하는 경우	이 위치로	DataSync는 다음을 복사할 수 있습니다
• NFS • Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용)	• Amazon S3	Amazon S3 사용자 메타데이터로서 복사할 수 있습니다. • 파일 및 폴더 수정 타임스탬프 • 파일 및 폴더 액세스 타임스탬프(DataSync는 최선의 노력으로만 이러한 작업을 수행 할 수 있음) • 사용자 ID 및 그룹 ID • POSIX 권한 Amazon S3 사용자 메타데이터에 저장된 파일 메타데이터

다음 위치 중 하나에서 복사하는 경우	이 위치로	DataSync는 다음을 복사할 수 있습니다
		는 AWS Storage Gateway을 사용하는 File Gateway에서 NFS와 상호 운용할 수 있습니다. File Gateway를 사용하면 온 프레미스 네트워크에서 DataSync가 Amazon S3로 복사한 데이터에 지연 시간이 짧게 액세스할 수 있습니다. 이 메타데이터는 Lustre용 FSx와도 상호 운용할 수 있습니다. DataSync가 이 메타데이터를 포함하는 객체를 다시 NFS 서버로 복사하는 경우, 파일 메타데이터가 복원됩니다. 메타데이터를 복원하려면 NFS 서버에 상향 조정된 권한을 부여해야 합니다. 자세한 설명은 NFS 파일 서버를 사용하여 AWS DataSync 전송 구성섹션을 참조하세요.

Amazon S3와 다른 객체 스토리지 사이에서

이러한 위치 사이에 복사하는 경우	DataSync는 다음을 복사할 수 있습니다

• 객체 스토리지
• Amazon S3
	• 사용자 정의 객체 메타데이터
	• 객체 태그
	• 시스템 정의 객체 메타데이터는 다음과 같습니다.
	  • Content-Disposition
	  • Content-Encoding
	  • Content-Language

• Microsoft Azure Blob Storage • Amazon S3	

이러한 위치 사이에 복사하는 경우	DataSync는 다음을 복사할 수 있습니다
	• Content-Type 참고: DataSync는 초기 전송 중에 모든 객체의 시스템 수준 메타데이터를 복사합니다. 변경된 데이터만 전송하도록 작업을 구성한 경우, 객체의 콘텐츠 또는 사용자 메타데이터도 수정되지 않는 한 DataSync는 후속 전송에서 시스템 메타데이터를 복사하지 않습니다. DataSync는 객체 액세스 제어 목록(ACL), 이전 객체 버전 또는 Last-Modified 키와 같은 다른 객체 메타데이터를 복사하지 않습니다.

Amazon S3와 HDFS 사이에서

이러한 위치 사이에 복사하는 경우	DataSync는 다음을
• Hadoop 분산 파일 시스템(HDFS) • Amazon S3	Amazon S3 사용자 메타데이터로서 복사할 수 있습니다. • 파일 및 폴더 수정 타임스탬프 • 파일 및 폴더 액세스 타임스탬프(DataSync는 최선의 노력으로만 이러한 작업을 수행 할 수 있음) • 사용자 ID 및 그룹 ID • POSIX 권한 HDFS는 UID 및 GID와 같은 숫자 식별자 대신, 문자열을 사용하여 파일 및 폴더 사용자 및 그룹 소유권을 저장합니다.

NFS 전송 시 복사된 메타데이터

다음 표에서는 NFS(네트워크 파일 시스템)를 사용하는 위치 간에 DataSync가 복사할 수 있는 메타데이터를 설명합니다.

이러한 위치 사이에 복사하는 경우	DataSync는 다음을 복사할 수 있습니다
• NFS • Amazon EFS • Amazon FSx for Lustre • Amazon FSx for OpenZFS • Amazon FSx for NetApp ONTAP (NFS 사용)	• 파일 및 폴더 수정 타임스탬프 • 파일 및 폴더 액세스 타임스탬프(DataSync는 최선의 노력으로만 이러한 작업을 수행 할 수 있음) • 사용자 ID(UID) 와 그룹 ID(GID) • POSIX 권한

SMB 전송 시 복사된 메타데이터

다음 표에서는 서버 메시지 블록(SMB)을 사용하는 위치 사이에서 DataSync가 복사할 수 있는 메타데이터를 설명합니다.

이러한 위치 사이에 복사하는 경우	DataSync는 다음을 복사할 수 있습니다
• SMB • Amazon FSx for Windows File Server • ONTAP용 FSx(SMB 사용)	• 파일 타임스탬프: 액세스 시간, 수정 시간 및 생성 시간 • 파일 소유자 보안 식별자(SID) • 표준 파일 속성: 읽기 전용(R), 아카이브(A), 시스템(S), 숨김(H), 압축(C), 컨텐츠 인덱싱되지 않음(I), 암호화된 파일(E), 임시(T), 오프라인(O), 스파스(P) DataSync는 아카이브(A), 컨텍스트 인덱싱된 속성(I)이 아닌 압축(C) 속성, 스파스(P), 임시(T) 속성을 최대한 복사하려고 시도합니다. 이러한 속성이 목적지에 적용되지 않으면 작업 검증 중에 무시됩니다.

이러한 위치 사이에 복사하는 경우	DataSync는 다음을 복사할 수 있습니다
	• NTFS 자유 재량적 액세스 제어 목록(DACL)은 객체에 액세스 권한을 부여할지 여부를 결정합니다. • NTFS 시스템 액세스 제어 목록(SACL)은 관리자가 보안 객체에 액세스하려는 시도를 로깅하는 데 사용됩니다. 참고: SMB 버전 1.0을 사용할 경우, SACL은 복사되지 않습니다. DACL과 SACL을 복사하려면 DataSync가 SMB를 사용하여 사용자 위치에 액세스하는 데 사용하는 Windows 사용자에게 특정 권한을 부여해야 합니다. 자세한 내용은 SMB, Windows File Server용 FSx 또는 ONTAP용 FSx를 위한 위치 만들기(전송 위치 유형에 따라 다름)를 참조하세요.

다른 전송 시나리오에서 복사된 메타데이터

DataSync는 이 스토리지 시스템들(대부분 메타데이터 구조가 다름) 간에 복제할 때 다음과 같은 방식으로 메타데이터를 처리합니다.

이 위치 중 하나에서 복사하는 경우	이 위치 중 한 곳으로	DataSync는 다음을 복사할 수 있습니다
• SMB • FSx for Windows File Server • ONTAP용 FSx(SMB 사용)	• Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용) • Amazon S3 • 객체 스토리지 • Azure Blob Storage	목적지 파일 시스템의 모든 파일 및 폴더 또는 목적지 S3 버킷의 객체에 대한 기본 POSIX 메타데이터입니다. 이 방법에는 기본 POSIX 사용자 ID 및 그룹 ID 값 사용이 포함됩니다. Windows 기반 메타데이터(예: ACL)는 보존되지 않습니다.

이 위치 중 하나에서 복사하는 경우	이 위치 중 한 곳으로	DataSync는 다음을 복사할 수 있습니다
	• NFS	
• 객체 스토리지 • Amazon S3 • Azure Blob Storage	• Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용)	목적지 파일 및 폴더에서의 기본 POSIX 메타데이터. 이 방법에는 기본 POSIX 사용자 ID 및 그룹 ID 값 사용이 포함됩니다.
• Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용)	• Azure Blob Storage	다음은 사용자 정의 메타데이터입니다. • 파일 및 폴더 수정 타임스탬프 • 파일 및 폴더 액세스 타임스탬프(DataSync는 최선의 노력으로만 이러한 작업을 수행 할 수 있음) • 사용자 ID 및 그룹 ID • POSIX 권한

이 위치 중 하나에서 복사하는 경우	이 위치 중 한 곳으로	DataSync는 다음을 복사할 수 있습니다
• HDFS	• Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용)	• 파일 및 폴더 수정 타임스탬프 • 파일 및 폴더 액세스 타임스탬프(DataSync는 최선의 노력으로만 이러한 작업을 수행 할 수 있음) • POSIX 권한 HDFS는 (UID 및 GID와 같은) 숫자 식별자보다는 오히려 문자열로 파일 및 폴더 사용자 및 그룹 소유권을 저장합니다. UID 및 GID의 기본값은 목적지 파일 시스템에 적용됩니다. 자세한 설명은 DataSync가 기본 POSIX 메타데이터를 적용하는 시기와 방법에 대한 이해섹션을 참조하세요.
• Amazon S3 • Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • FSx for Windows File Server • OnTAP용 FSx	• HDFS	소스 위치의 파일 및 폴더 타임스탬프. 파일 또는 폴더 소유자는 HDFS 전송 위치를 만들 때 지정한 HDFS 사용자 또는 Kerberos 보안 주체를 기반으로 설정됩니다. Hadoop 클러스터의 그룹 매핑 구성에 따라 그룹이 결정됩니다.

이 위치 중 하나에서 복사하는 경우	이 위치 중 한 곳으로	DataSync는 다음을 복사할 수 있습니다
• Amazon S3 • Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용) • 객체 스토리지 • NFS • HDFS	• SMB • FSx for Windows File Server • ONTAP용 FSx(SMB 사용)	소스 위치의 파일 및 폴더 타임스탬프. 소유권은 Amazon FSx 또는 SMB 공유에 액세스하기 위해 DataSync에서 지정된 Windows 사용자를 기반으로 설정됩니다. 권한은 상위 디렉토리로부터 상속됩니다.
• Azure Blob Storage	• FSx for Windows File Server • ONTAP용 FSx(SMB 사용)	

DataSync가 기본 POSIX 메타데이터를 적용하는 시기와 방법에 대한 이해

DataSync는 다음과 같은 경우에 기본 POSIX 메타데이터를 적용합니다.

- 사용자 전송의 소스 및 대상 위치에 유사한 메타데이터 구조가 없는 경우
- 소스 위치에 메타데이터가 누락된 경우

다음 표는 DataSync가 이러한 유형의 전송 중에 기본 POSIX 메타데이터를 적용하는 방법을 설명합니다.

소스	Destination	파일 권한	폴더 권한	UID	GID
• Amazon S3[1] • 객체 스토리지 [1] • Microsoft Azure Blob Storage 1	• Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx	0755	0755	65534	65534

소스	Destination	파일 권한	폴더 권한	UID	GID
	• ONTAP용 FSx(NFS 사용) • NFS				
• SMB	• Amazon S3 • 객체 스토리지 • Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용) • NFS	0644	0755	65534	65534
• HDFS	• Amazon EFS • FSx for Lustre • FSx OpenZFS용 FSx • ONTAP용 FSx(NFS 사용) • NFS	0644	0755	65534	65534

[1] 이전에 DataSync에 의해 적용한 메타데이터가 객체에 없는 경우.

에서 복사한 링크 및 디렉터리 AWS DataSync

AWS DataSync 는 전송과 관련된 스토리지 위치에 따라 하드 링크, 심볼 링크 및 디렉터리를 다르게 처리합니다.

하드 링크

DataSync가 몇 가지 일반적인 전송 시나리오에서 하드 링크를 처리하는 방법은 다음과 같습니다.

- NFS 파일 서버, Lustre용 FSx, OpenZFS용 FSx, ONTAP용 FSx(NFS 사용) 및 Amazon EFS 간에 전송하는 경우 하드 링크가 보존됩니다.
- Amazon S3로 전송할 때 하드 링크로 참조되는 각 기본 파일은 한 번만 전송됩니다. 증분 전송 중에는 S3 버킷에 별도의 객체가 생성됩니다. Amazon S3에서 하드 링크가 변경되지 않은 경우, NFS 파일 서버, Lustre 용 FsX, OpenZFS용 FSx, ONTAP용 FSx(NFS 사용) 또는 Amazon EFS 파일 시스템으로 전송될 때 하드링크는 올바르게 복원됩니다.
- Microsoft Azure Blob Storage로 전송할 때 하드 링크로 참조되는 각 기본 파일은 한 번만 전송됩니다. 증분 전송 시 원본에 새 참조가 있는 경우 blob 저장소에 별도의 객체가 생성됩니다. Azure Blob Storage에서 전송할 때 DataSync는 하드 링크를 개별 파일인 것처럼 전송합니다.
- SMB 파일 서버, Windows File Server용 FSx 및 ONTAP용 FSx(SMB 사용) 간에 전송하는 경우 하드 링크는 지원되지 않습니다. 이러한 상황에서 DataSync가 하드 링크와 마주치게 되면, 전송 작업이 완료되고 오류가 발생합니다. 자세한 내용은 CloudWatch 로그를 확인하세요.
- HDFS로 전송할 때 하드 링크는 지원되지 않습니다. CloudWatch 로그에는 이러한 링크가 건너뛰기 한 것으로 표시됩니다.

심볼 링크

DataSync가 몇 가지 일반적인 전송 시나리오에서 심볼 링크를 처리하는 방법은 다음과 같습니다.

- NFS 파일 서버, Lustre용 FSx, OpenZFS용 FSx, ONTAP용 FSx(NFS 사용) 및 Amazon EFS 간에 전송하는 경우 심볼 링크가 보존됩니다.
- Amazon S3로 전송할 때 링크 대상 경로가 Amazon S3 객체에 저장됩니다. NFS 파일 서버, Lustre 용 FsX, OpenZFS용 FSx, ONTAP용 FSx (NFS 사용) 또는 Amazon EFS 파일 시스템으로 전송될 때 링크는 올바르게 복원됩니다.
- Azure Blob Storage로 전송할 때 심볼 링크는 지원되지 않습니다. CloudWatch 로그에는 이러한 링크가 건너뛰기 한 것으로 표시됩니다.

- SMB 파일 서버, Windows File Server의 경우 FSx 및 ONTAP용 FSx(SMB 사용) 간에 전송하는 경우 심볼 링크는 지원되지 않습니다. DataSync는 심볼 링크 자체를 전송하지 않고 대신 심볼 링크에서 참조하는 파일을 전송합니다. 중복 파일을 인식하고 심볼 링크를 사용하여 중복 제거하려면 대상 파일 시스템에서 중복 제거를 구성해야 합니다.
- HDFS로 전송할 때 심볼 링크는 지원되지 않습니다. CloudWatch 로그에는 이러한 링크가 건너뛰기 한 것으로 표시됩니다.

디렉터리

일반적으로 DataSync는 스토리지 시스템 간 전송 시 디렉토리를 보존합니다. 이는 다음과 같은 경우에는 해당되지 않습니다.

- Amazon S3로 전송할 때 디렉터리는 접두사가 있고 포워드 슬래시(/)로 끝나는 빈 객체로 표시됩니다.
- 계층적 네임스페이스 없이 Azure Blob Storage로 전송할 때는 디렉터리가 존재하지 않습니다. 디렉터리처럼 보이는 것은 개체 이름의 일부일 뿐입니다.

파일, 객체 및 메타데이터 처리 방법 구성

위치 간에 전송할 때가 파일, 객체 및 관련 메타데이터를 AWS DataSync 처리하는 방법을 구성할 수 있습니다.

예를 들어 반복 전송의 경우 위치를 동기화하기 위해 대상의 파일을 원본의 변경 내용으로 덮어쓰고 싶을 수 있습니다. 파일 및 폴더에 대한 POSIX 권한, 객체와 관련된 태그, 액세스 제어 목록(ACL) 과 같은 속성을 복사할 수 있습니다.

전송 모드 옵션

DataSync가 초기 복사 후 변경된 데이터(메타데이터 포함)만 전송할지 아니면 작업을 실행할 때마다 모든 데이터를 전송할지를 구성할 수 있습니다. 반복 전송을 계획한다면 이전 작업 실행 이후 변경된 내용만 전송하는 것이 좋을 수 있습니다.

콘솔 내 옵션	API 내 옵션	설명
변경된 데이터만 전송	TransferMode를 CHANGED(으)로 설정	최초 전체 전송 후 DataSync는 소스 위치와 대상 위치 간에 서로 다른 데이터와 메타데이터만 복사합니다.

콘솔 내 옵션	API 내 옵션	설명
모든 데이터 전송	TransferMode를 ALL(으)로 설정	DataSync는 위치 간의 차이를 비교하지 않고 소스의 모든 데이터를 대상으로 복사합니다.

파일 및 객체 처리 옵션

DataSync가 대상 위치의 파일 또는 객체를 처리하는 방식 중 일부를 제어할 수 있습니다. 예를 들어 DataSync는 소스에는 없는 대상 내 파일을 삭제할 수 있습니다.

콘솔 내 옵션	API 내 옵션	설명
삭제된 파일 유지	PreserveDeletedFiles	DataSync가 소스에는 존재하지 않는 파일이나 객체를 대상 위치에 유지할지 여부를 지정합니다. Amazon S3 버킷에서 객체를 삭제하도록 작업을 구성하는 경우, 특정 스토리지 클래스에 대한 최소 스토리지 기간 요금이 발생할 수 있습니다. 자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항섹션을 참조하세요. **Warning** 대상의 데이터를 삭제하면서, 동시에 모든 데이터를 전송하도록 작업을 구성할 수는 없습니다. 모든 데이터를 전송할 때 DataSync는 목적지 위치를 스캔하지

콘솔 내 옵션	API 내 옵션	설명
		않으므로 무엇을 삭제해야 할지 모릅니다.
파일 덮어쓰기	OverwriteMode	소스 데이터 또는 메타데이터가 변경되었을 때 DataSync가 대상 위치의 데이터를 수정할지 여부를 지정합니다. 데이터를 덮어쓰도록 작업을 구성하지 않으면 소스 데이터가 다르더라도 대상 데이터를 덮어쓰지 않습니다. 태스크에서 객체를 덮어쓰는 경우, 특정 스토리지 클래스(예: 검색 또는 조기 삭제)에 대한 추가 요금이 발생할 수 있습니다. 자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항섹션을 참조하세요.

메타데이터 처리 옵션

DataSync는 데이터 전송 중에 파일 또는 객체 메타데이터를 보존할 수 있습니다. DataSync가 보존할 수 있는 메타데이터는 관련된 스토리지 시스템과 해당 시스템이 유사한 메타데이터 구조를 사용하는지 여부에 따라 달라집니다.

작업을 구성하기 전에 DataSync가 소스와 대상 위치 간 전송 시 메타데이터 및 특수 파일을 처리하는 방법을 이해해야 합니다.

> **Important**
>
> DataSync는 Google Cloud Storage 및 IBM Cloud 객체 스토리지와 같은 특정 타사 클라우드 스토리지 시스템으로 보내거나 받는 양방향 전송을 지원하며, 이는 S3과 완전히 호환되지는 않는 방식으로 시스템 메타데이터를 처리합니다. 이러한 전송을 위해 DataSync는 최선을 다해 `ContentType`, `ContentEncoding`, `ContentLanguage`, `CacheControl`와 같은 메타데이

터 속성을 복사하고자 시도합니다. 대상 스토리지 시스템이 이러한 속성을 적용하지 않으면 해당 속성은 작업 확인 중에 무시됩니다.

콘솔 내 옵션	API 내 옵션	설명
소유권 복사	GID 및 UID	DataSync는 파일 소유자의 그룹 ID 및 파일 소유자의 사용자 ID와 같은 POSIX 파일 및 폴더 소유권의 복사 여부를 지정합니다.
복사 권한	PosixPermissions	DataSync는 파일 및 폴더에 대한 POSIX 권한을 소스에서 대상으로 복사할지 여부를 지정합니다.
타임스탬프 복사	Atime 및 Mtime	DataSync는 타임스탬프 메타데이터를 소스에서 대상으로 복사할지 여부를 지정합니다. 이 옵션은 작업을 두 번 이상 실행해야 하는 경우에 필요합니다.
객체 태그 복사	ObjectTags	DataSync는 객체 스토리지 시스템 간 전송 시 객체와 관련된 태그 보존 여부를 지정합니다.
소유권, DACL 및 SACL 복사	SecurityDescriptorCopyFlags를 `OWNER_DACL_SACL` (으)로 설정	DataSync는 다음을 복사합니다. • 객체 소유자 • NTFS 자유 재량적 액세스 제어 목록(DACL)은 객체에 액세스 권한을 부여할지 여부를 결정합니다.

콘솔 내 옵션	API 내 옵션	설명
		• NTFS 시스템 액세스 제어 목록(SACL)은 관리자가 보안 객체에 액세스하려는 시도를 로깅하는 데 사용됩니다. 참고: SMB 버전 1.0을 사용할 경우, SACL은 복사되지 않습니다. DACL과 SACL을 복사하려면 DataSync가 SMB를 사용하여 사용자 위치에 액세스하는 데 사용하는 Windows 사용자에게 특정 권한을 부여해야 합니다. 자세한 내용은 SMB, Windows File Server용 FSx 또는 ONTAP 용 FSx를 위한 위치 생성(전송 위치 유형에 따라 다름)을 참조하십시오.
소유권 및 DACL 복사	SecurityDescriptorCopyFlags를 OWNER_DACL (으)로 설정	DataSync는 다음을 복사합니다. • 객체 소유자 • 자유 재량적 액세스 제어 목록(DACL)은 객체에 액세스 권한을 부여할지 여부를 결정합니다. 이 옵션을 선택하면, DataSync는 SACL을 복사하지 않습니다.

콘솔 내 옵션	API 내 옵션	설명
소유권이나 ACL을 복사하지 마세요.	SecurityDescriptorCopyFlags를 NONE(으)로 설정	DataSync는 소유권 또는 권한 데이터를 복사하지 않습니다. DataSync가 대상 위치에 쓰는 객체가 DataSync가 대상에 액세스할 수 있도록 보안 인증을 제공한 사용자가 소유합니다. 대상 객체 권한은 대상 서버에 구성된 권한에 따라 결정됩니다.

파일, 객체, 메타데이터 처리 옵션 구성

전송 작업을 생성, 편집, 시작할 때 DataSync가 파일, 객체, 메타데이터를 처리하는 방법을 구성할 수 있습니다.

DataSync 콘솔 사용

다음 지침에서는 작업 생성 시 파일, 객체, 메타데이터 처리 옵션을 구성하는 방법을 설명합니다.

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 전송 모드의 경우, 다음 옵션 중 하나를 선택합니다.

   - 변경된 데이터만 전송
   - 모든 데이터 전송

   이러한 옵션에 대한 자세한 내용은 전송 모드 옵션 섹션을 참조하세요.
5. DataSync가 소스에 없는 대상 위치의 파일 또는 객체를 유지하도록 하려면 삭제된 파일 유지를 선택합니다.

이 옵션을 선택하지 않고 사용자의 태스크가 Amazon S3에서 객체를 삭제하는 경우, 특정 스토리지 클래스에 대한 최소 스토리지 기간 요금이 발생할 수 있습니다. 자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항섹션을 참조하세요.

> **Warning**
>
> 이 옵션을 선택 취소하고 모든 데이터 전송을 활성화할 수는 없습니다. 모든 데이터를 전송할 때 DataSync는 목적지 위치를 스캔하지 않으므로 무엇을 삭제해야 할지 모릅니다.

6. 소스 데이터 또는 메타데이터가 변경되었을 때 DataSync가 대상 위치의 데이터를 수정하도록 하려면 파일 덮어쓰기를 선택합니다.

   태스크에서 객체를 덮어쓰는 경우, 특정 스토리지 클래스(예: 검색 또는 조기 삭제) 에 대한 추가 요금이 발생할 수 있습니다. 자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항섹션을 참조하세요.

   이 옵션을 선택하지 않으면, 소스 데이터가 다르더라도 대상 데이터를 덮어쓰지 않습니다.

7. 전송 옵션에서 DataSync가 메타데이터를 처리하는 방법을 선택합니다. 이러한 옵션에 대한 자세한 내용은 메타데이터 처리 옵션을 참조하세요.

> **Important**
>
> 콘솔에 표시되는 옵션은 작업의 소스 및 대상 위치에 따라 달라집니다. 이러한 옵션을 보려면 추가 설정을 확장해야 할 수 있습니다.

- 소유권 복사
- 복사 권한
- 타임스탬프 복사
- 객체 태그 복사
- 소유권, DACL 및 SACL 복사
- 소유권 및 DACL 복사
- 소유권이나 ACL을 복사하지 마세요.

DataSync API 사용

다음 작업 중 하나와 함께 `Options` 파라미터를 사용하여 파일, 객체, 메타데이터 처리 옵션을 구성할 수 있습니다.

- CreateTask
- StartTaskExecution
- UpdateTask

가 데이터 무결성을 AWS DataSync 확인하는 방법 구성

전송 중에는 체크섬 확인을 AWS DataSync 사용하여 위치 간에 복사하는 데이터의 무결성을 확인합니다. 전송이 끝날 때 추가 확인을 수행하도록 DataSync를 구성할 수도 있습니다.

데이터 확인 옵션

다음 정보를 사용하면 DataSync가 이러한 추가 검사를 수행할지 여부와 방법을 결정하는 데 도움이 됩니다.

콘솔 옵션	API 옵션	설명
전송된 데이터만 확인(권장)	VerifyMode를 `ONLY_FILES_TRANSFERRED` (으)로 설정	DataSync는 소스 위치에서 전송된 데이터(메타데이터 포함)의 체크섬을 계산합니다. 전송이 끝날 때, DataSync가 이 체크섬을 대상에서의 동일한 데이터에 대해 계산된 체크섬과 비교합니다. S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스로 전송하는 경우, 이 옵션을 사용하는 것이 좋습니다. 자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항 단원을 참조하십시오.

콘솔 옵션	API 옵션	설명
모든 데이터 확인	VerifyMode를 POINT_IN_TIME_CONSISTENT (으)로 설정	전송 종료 시 DataSync는 전체 소스와 대상을 검사하여 두 위치가 완전히 동기화되었는지 확인합니다. **Note** 작업이 확장 모드를 사용하는 경우 지원되지 않습니다. 매니페스트를 사용하는 경우 DataSync는 매니페스트에 나열된 항목만 스캔하고 확인합니다. S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스로 전송하는 경우 이 옵션을 사용할 수 없습니다. 자세한 내용은 Amazon S3 전송 시 스토리지 클래스 고려 사항 단원을 참조하십시오.
전송 후 데이터 확인 안 함	VerifyMode를 NONE(으)로 설정	DataSync는 전송 중에만 데이터 무결성 검사를 수행합니다. 다른 옵션과 달리 전송이 끝날 때 추가 확인은 없습니다.

데이터 확인 구성

작업을 생성하거나, 작업을 업데이트하거나, 작업 실행을 시작할 때 데이터 확인 옵션을 구성할 수 있습니다.

DataSync 콘솔 사용

다음 지침에서는 태스크를 생성 시 데이터 확인 옵션을 구성하는 방법을 설명합니다.

콘솔을 사용하여 데이터 검사를 구성하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 확인에서 다음 중 하나를 선택합니다.

   - 전송된 데이터만 확인(권장)
   - 모든 데이터 확인
   - 전송 후 데이터 확인 안 함

DataSync API 사용

다음 작업을 통해 `VerifyMode` 파라미터를 사용하여 DataSync가 데이터를 검사하는 방법을 구성할 수 있습니다.

- CreateTask
- UpdateTask
- StartTaskExecution

AWS DataSync 작업에 대한 대역폭 제한 설정

AWS DataSync 작업 및 각 실행에 대한 네트워크 대역폭 제한을 구성할 수 있습니다.

태스크의 대역폭 제한

태스크를 생성, 편집 또는 시작할 때 대역폭 제한을 설정합니다.

DataSync 콘솔 사용

다음 지침은 태스크 생성 시 태스크의 대역폭 제한을 구성하는 방법을 설명합니다.

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 대역폭 제한에서 다음 중 하나를 선택합니다.

   - 각 태스크 실행에 대하여 모든 사용 가능한 네트워크 대역폭을 사용하려면 사용하기 가능 을 선택합니다.
   - 대역폭 제한 설정(MiB/s) 을 선택하고 DataSync가 각 태스크 실행에 사용할 최대 대역폭을 입력합니다.

DataSync API 사용

다음 태스크 중 하나에서 `BytesPerSecond`파라미터를 사용하여 태스크의 대역폭 제한을 구성할 수 있습니다.

- CreateTask
- UpdateTask
- StartTaskExecution

태스크 실행을 위한 대역폭 조절

실행 중이거나 대기 중인 태스크 실행의 대역폭 제한을 수정할 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 탐색 창에서 데이터 전송을 확장한 다음 태스크를 선택합니다.
3. 태스크를 선택한 다음 기록을 선택하여 태스크 실행을 확인합니다.
4. 수정할 태스크 실행을 선택한 후 편집을 선택합니다.
5. 대화 상자에서 다음 중 하나를 수행합니다.

   - 태스크 실행에 모든 사용 가능한 네트워크 대역폭을 사용하려면 사용하기 가능을 선택합니다.
   - 대역폭 제한 설정(MiB/s)을 선택하고 DataSync가 태스크 실행에 사용할 최대 대역폭을 입력합니다.
6. 변경 사항 저장을 선택합니다.

새 대역폭 제한은 60초 이내에 적용됩니다.

DataSync API 사용

UpdateTaskExecution을 가지고 BytesPerSecond파라미터를 사용하여 실행 중이거나 대기중인 태스크 실행에 대한 대역폭 제한을 수정할 수 있습니다.

AWS DataSync 작업 실행 시 예약

스토리지 위치 간에 데이터를 정기적으로 전송하도록 AWS DataSync 작업을 설정할 수 있습니다.

DataSync 작업 예약 작동 방식

예약된 DataSync 작업은 사용자가 지정한 빈도(최소 1시간 간격)로 실행됩니다. Cron 또는 Rate 표현식을 사용하여 작업 일정을 생성할 수 있습니다.

> **Important**
>
> 1시간 이내의 간격으로 작업이 실행되도록 예약할 수 없습니다.

cron 표현식 사용

특정 시간 및 날짜에 실행되는 작업 일정에 Cron 표현식을 사용합니다. 예를 들어 일요일과 수요일 오후 12:00 UTC에 AWS CLI에서 실행되는 작업 일정을 구성하는 방법은 다음과 같습니다.

```
cron(0 12 ? * SUN,WED *)
```

Rate 표현식 사용

12시간마다와 같이 정기적으로 실행되는 작업 일정에 Rate 표현식을 사용합니다. 예를 들어 12시간마다 AWS CLI에서 실행되는 작업 일정을 구성하는 방법은 다음과 같습니다.

```
rate(12 hours)
```

> **Tip**
>
> Cron 표현식 및 Rate 표현식 구문에 대한 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

DataSync 작업 일정 생성

DataSync 콘솔, AWS CLI 또는 DataSync API를 사용하여 작업 실행 빈도를 예약할 수 있습니다.

DataSync 콘솔 사용

다음 지침은 작업을 생성할 때 일정을 설정하는 방법을 설명합니다. 작업을 편집할 경우 나중에 일정을 수정할 수 있습니다.

콘솔에서 일부 예약 옵션을 사용하면 작업이 실행되는 정확한 시간(예: 매일 오후 10시 30분)을 지정할 수 있습니다. 이러한 옵션에 시간을 포함하지 않으면 작업은 작업을 생성(또는 업데이트)하는 시점에 실행됩니다.

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 일정 빈도에서 다음 중 하나를 수행합니다.
   - 작업이 일정에 따라 실행되지 않게 하려면 예약되지 않음을 선택합니다.
   - 시간별을 선택한 다음 작업을 실행할 시간 중 분을 선택합니다.
   - 일별을 선택하고 작업을 실행할 UTC 시간을 입력합니다.
   - 주별 및 요일을 선택하고 작업을 실행할 UTC 시간을 입력합니다.
   - 요일을 선택하고 특정 요일을 선택한 다음 작업을 실행할 UTC 시간을 HH:MM 형식으로 입력합니다.
   - 사용자 지정을 선택한 다음 Cron 표현식 또는 Rate 표현식을 선택합니다. 최소 1시간 간격으로 작업 일정을 입력합니다.

AWS CLI 사용

`--schedule` 파라미터를 `create-task`, `update-task` 또는 `start-task-execution` 명령과 함께 사용하여 DataSync 작업의 일정을 생성할 수 있습니다.

다음 지침은 `create-task` 명령을 사용하여 이 작업을 수행하는 방법을 설명합니다.

1. 다음 `create-task`명령을 복사합니다.

```
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. `--source-location-arn` 파라미터에서 데이터를 전송하는 소스 위치의 Amazon 리소스 이름(ARN)을 지정합니다.
3. `--destination-location-arn` 파라미터에서 데이터를 전송하는 대상 위치의 ARN을 지정합니다.
4. `--schedule` 파라미터에서 일정에 대한 Cron 또는 Rate 표현식을 지정합니다.

   이 예제에서 Cron 표현식 *`cron(0 12 ? * SUN,WED *)`*은 매주 일요일과 수요일 오후 12:00 UTC에 실행되는 작업 일정을 설정합니다.
5. `create-task` 명령을 실행하여 일정이 있는 작업을 생성합니다.

DataSync 작업 일정 일시 중지

DataSync 작업 일정을 일시 중지해야 하는 상황이 있을 수 있습니다. 예를 들어 작업 문제를 해결하거나 스토리지 시스템에서 유지 관리를 수행하려면 반복 전송을 일시적으로 비활성화해야 할 수 있습니다.

DataSync는 다음과 같은 이유로 작업 일정을 자동으로 비활성화할 수 있습니다.

- 동일한 오류로 작업이 반복적으로 실패합니다.
- 작업에서 사용 중인 AWS 리전을 비활성화합니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 작업을 선택합니다.
3. 일정을 일시 중지하려는 작업을 선택한 다음 편집을 선택합니다.
4. 일정에서 일정 활성화를 끕니다. 변경 사항 저장을 선택합니다.

AWS CLI 사용

1. 다음 `update-task`명령을 복사합니다.

```
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. `--task-arn` 파라미터에서 일정을 일시 중지하려는 작업의 ARN을 지정합니다.
3. `--schedule` 파라미터에 관하여 다음을 수행합니다.
   - `ScheduleExpression`에서 일정에 대한 Cron 또는 Rate 표현식을 지정합니다.

     이 예제에서 표현식 *`cron(0 12 ? * SUN,WED *)`*은 매주 일요일과 수요일 오후 12:00 UTC에 실행되는 작업 일정을 설정합니다.
   - `Status`에서 작업 일정을 일시 중지하도록 `DISABLED`로 지정합니다.
4. `update-task` 명령을 실행합니다.
5. 일정을 재개하려면 `Status`를 `ENABLED`로 설정하여 동일한 `update-task` 명령을 실행합니다.

DataSync 작업 일정 상태 확인

DataSync 작업 일정이 활성화되어 있는지 확인할 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 작업을 선택합니다.

3. 일정 열에서 작업의 일정이 활성화되어 있는지 비활성화되어 있는지 확인합니다.

AWS CLI 사용

1. 다음 `describe-task`명령을 복사합니다.

```
aws datasync describe-task \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

2. `--task-arn` 파라미터에서 정보를 원하는 작업의 ARN을 지정합니다.
3. `describe-task` 명령을 실행합니다.

일정을 포함하여 작업에 대한 세부 정보를 제공하는 응답을 받습니다. (다음 예제는 주로 작업 일정 구성에 초점을 맞추고 전체 `describe-task` 응답을 표시하지 않습니다.)

이 예제는 작업의 일정이 수동으로 비활성화되었음을 보여줍니다. DataSync `SERVICE`에 의해 일정이 비활성화된 경우 작업이 계속 실패하는 이유를 이해하는 데 도움이 되는 `DisabledReason`에 대한 오류 메시지가 표시됩니다. 자세한 내용은 ??? 섹션을 참조하세요.

```
{
    "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."
    },
    ...
}
```

AWS DataSync 작업에 태그 지정

태그는 AWS DataSync 리소스를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다. 각 DataSync 태스크 및 태스크 실행에 최대 50개의 태그를 추가할 수 있습니다.

예를 들어, 대규모 데이터 마이그레이션을 위한 태스크를 생성하고 해당 태스크에 **`Project`**키와 값**`Large Migration`**을 태그할 수 있습니다. 마이그레이션을 더 체계적으로 구성하려면 한 번의 태

스크 실행에 **`Transfer Date`**키와 값을 태그로 지정할 수 있습니다(**`May 2021`**후속 태그 실행에는 **`June 2021`**, **`July 2021`**등의 태그가 지정될 수 있음).

DataSync 작업 태그 지정

태스크를 생성할 때만 DataSync 태스크에 태그를 지정할 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 설정 구성 페이지에서 새 태그 추가를 선택하여 작업에 태그를 지정합니다.

사용 AWS CLI

1. 다음 `create-task`명령을 복사합니다.

```
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. 명령에서 다음 파라미터를 지정합니다.

   - `--source-location-arn`- 전송할 때 소스 위치의 Amazon 리소스 이름(ARN) 을 지정합니다.
   - `--destination-location-arn` – 전송할 대상 위치의 ARN을 지정합니다.
   - `--tags` – 태스크에 적용할 태그를 지정합니다.

     태그가 두 개 이상인 경우 각 키-값 쌍을 공백으로 구분하세요.
3. (선택 사항) 전송 시나리오에 적합한 다른 파라미터를 지정하세요.

   `--options`목록의 경우, create-task 명령을 참조하세요.
4. `create-task` 명령을 실행합니다.

방금 생성한 태스크를 보여주는 응답을 받게 됩니다.

```
{
    "TaskArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

이 태스크에 추가한 태그를 보려면 list-tags-for-resource 명령을 사용할 수 있습니다.

DataSync 작업 실행 태그 지정

DataSync 태스크의 각 실행에 태그를 지정할 수 있습니다.

태스크에 이미 태그가 있는 경우, 태스크 실행 시 태그 사용에 관한 다음 사항을 기억하세요.

- 콘솔에서 태스크를 시작하면 사용자가 생성한 태그가 태스크 실행에 자동으로 적용됩니다. 그러나 `aws:`로 시작하는 시스템 생성 태그는 적용되지 않습니다.
- DataSync API 또는를 사용하여 작업을 시작하면 AWS CLI해당 태그가 작업 실행에 자동으로 적용되지 않습니다.

DataSync 콘솔 사용

태스크 실행에서 태그를 추가, 편집 또는 제거하려면 우선 적용 옵션을 사용하여 태스크를 시작해야 합니다.

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 태스크를 선택합니다.
3. 작업을 선택합니다.
4. 시작을 선택하고, 다음 옵션 중 하나를 선택합니다.
   - 기본값으로 시작 - 태스크과 관련된 모든 태그를 적용합니다.
   - 우선 적용 옵션으로 시작 - 이 특정 태스크 실행에 대한 태그를 추가, 편집 또는 제거할 수 있습니다.

사용 AWS CLI

1. 다음 `start-task-execution`명령을 복사합니다.

```
aws datasync start-task-execution \
    --task-arn 'arn:aws:datasync:region:account-id:task/task-id' \
    --tags Key=tag-key,Value=tag-value
```

2. 명령에서 다음 파라미터를 지정합니다.

   - `--task-arn`- 시작하려는 태스크의 ARN을 지정합니다.
   - `--tags`— 이 태스크 실행에 적용할 태그를 지정합니다.

     태그가 두 개 이상인 경우 각 키-값 쌍을 공백으로 구분하세요.

3. (선택 사항) 사용자의 상황 적합한 다른 파라미터를 지정하십시오.

   자세한 내용은start-task-execution 단원을 참조하십시오.

4. `start-task-execution` 명령을 실행합니다.

   방금 시작한 태스크를 보여주는 응답을 받게 됩니다.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

이 태스크에 추가한 태그를 보려면 list-tags-for-resource 명령을 사용할 수 있습니다.

데이터 전송 작업 시작

AWS DataSync전송 태스크를 생성하고 나면 데이터 이동을 시작할 수 있습니다. 각 태스크를 운영하는 것을 태스크 실행이라고 합니다. 작업 실행 중 발생하는 상황에 대한 자세한 내용은 DataSync가 파일, 객체, 디렉터리를 전송하는 방법을(를) 참조하세요.

> **Important**
>
> Amazon S3 위치와 데이터를 주고받을 계획이라면 시작하기 전에 DataSync가 S3 요청 요금에 미치는 영향 및 DataSync 요금 페이지를 검토하세요.

태스크 시작하

태스크를 생성하고 나면 바로 데이터 이동을 시작할 수 있습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송 확장한 다음, 태스크를 선택합니다.
3. 실행하려는 태스크를 선택합니다.

   태스크가 사용 가능 상태인지 확인하세요. 여러 태스크를 선택할 수도 있습니다.
4. 실행를 선택하고, 다음 옵션 중 하나를 선택합니다.

   - 시작 - 태스크(또는 둘 이상을 선택한 경우 태스크)를 실행합니다.
   - 우선 적용 옵션으로 시작 - 데이터 이동을 시작하기 전에 일부 태스크 설정을 수정할 수 있습니다. 준비가 되면, 시작을 선택합니다.
5. 실행 세부 정보 보기 를 선택하여 실행중인 태스크 실행에 대한 세부 정보를 확인합니다.

AWS CLI 사용

DataSync 작업을 시작하려면 실행하려는 작업의 Amazon 리소스 이름(ARN)을 지정하기만 하면 됩니다. 다음은 `start-task-execution`명령의 예입니다.

```
aws datasync start-task-execution \
    --task-arn 'arn:aws:datasync:region:account-id:task/task-id'
```

다음 예제에서는 작업의 기본 설정과 다른 몇 가지 설정을 사용하여 작업을 시작합니다.

```
aws datasync start-task-execution \
    --override-options VerifyMode=NONE,OverwriteMode=NEVER,PosixPermissions=NONE
```

이 명령은 다음 예제와 유사한 작업 실행에 대한 ARN을 반환합니다.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:209870788375:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

> **Note**
>
> 각 에이전트는 작업을 한 번에 하나씩 실행할 수 있습니다.

DataSync API 사용

StartTaskExecution을 사용하여 태스크를 시작할 수 있습니다. DescribeTaskExecution 태스크를 사용하면 실행중인 태스크 실행에 대한 세부 정보를 가져올 수 있습니다.

일단 시작되면 DataSync가 데이터를 복사할 때 작업 실행 상태를 확인할 수 있습니다. 필요한 경우 태스크 실행의 대역폭을 제한할 수도 있습니다.

태스크 실행 상태

DataSync 태스크를 시작하면 다음과 같은 상태가 표시될 수 있습니다. (작업 상태는 작업 실행 상태와 다릅니다.)

콘솔 상태	API 상태	설명
대기열	QUEUED	다른 작업 실행이 실행 중이며 동일한 DataSync 에이전트를 사용하고 있습니다. 자세한 내용은 작업이 대기열에 있는 시점 파악 섹션을 참조하세요.
실행	LAUNCHING	DataSync는 작업 실행을 초기화합니다. 이 상태는 일반적으로 빠르게 지나가지만, 최대 몇 분이 소요될 수 있습니다.
시작됨	LAUNCHED	DataSync가 작업 실행을 시작했습니다.
준비 중	PREPARING	DataSync는 전송이 필요한 데이터를 결정합니다. 이 단계는 두 위치의 파일, 객체, 디렉터리 수와 작업 구성 방식에 따라 단 몇 분에서 몇 시간, 또는 그 이상이 걸릴 수 있습니다. 준비 작업 방식 또한 작업 모드에 따라 달라집니다. 자세한 내용은 DataSync가 데이터 전송을 준비하는 방법 섹션을 참조하세요.

콘솔 상태	API 상태	설명
전송 중	TRANSFERRING	DataSync는 실제 데이터 전송을 수행합니다.
검사 중	VERIFYING	DataSync는 전송이 끝나면 데이터의 무결성을 확인합니다.
Success	SUCCESS	작업 실행에 성공했습니다.
취소 중	CANCELLING	작업 실행이 취소되는 중입니다.
오류	ERROR	작업 실행에 실패했습니다.

작업이 대기열에 있는 시점 파악

여러 작업을 실행할 때(예: 대규모 데이터세트를 전송하는 경우) DataSync는 시리즈로 실행되도록 작업을 대기열에 넣을 수 있습니다(선입선출). 이러한 상황이 발생하는 몇 가지 예제는 다음과 같습니다.

- 동일한 DataSync 에이전트를 사용하는 서로 다른 작업을 실행합니다. 동일한 에이전트를 여러 작업에 사용할 수 있지만 에이전트는 한 번에 하나의 작업만 실행할 수 있습니다.
- 작업 실행이 진행 중이며 다른 필터 또는 매니페스트를 사용하여 동일한 작업의 추가 실행을 시작합니다.

각 예제에서 대기 중인 작업은 앞에 있는 작업이 완료될 때까지 시작되지 않습니다.

작업 실행 취소

실행 중이거나 대기 중인 작업 실행을 모두 중지할 수 있습니다.

콘솔을 사용하여 작업 실행을 취소하려면

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 태스크를 선택합니다.
3. 모니터링하고자 하는 실행 중인 태스크의 태스크 ID를 선택합니다.

   태스크 상태는 실행 중이어야 합니다.
4. 태스크 실행을 보려면 기록을 선택합니다.

5. 중지하려는 태스크 실행을 선택한 후 중지를 선택합니다.
6. 대화 상자에서 중지를 선택합니다.

DataSync API를 사용하여 실행 중이거나 대기중인 태스크를 취소하려면 CancelTaskExecution을 참조하세요.

멈춘 작업 자동 취소

때때로 실행 중인 DataSync 작업 실행이 멈추기도 합니다.

AWS DataSync 전송 모니터링

모니터링은 AWS DataSync 전송 활동의 신뢰성과 성능을 유지하는 데 중요한 역할을 합니다. 발생하는 오류를 보다 쉽게 디버깅할 수 있도록 모니터링 데이터를 수집하는 것이 좋습니다. 하지만 DataSync 모니터링을 시작하기 전에 다음 질문에 대한 답변을 포함하는 모니터링 계획을 작성하십시오.

- 모니터링의 목표
- 모니터링할 리소스
- 이러한 리소스를 모니터링하는 빈도
- 사용할 모니터링 도구
- 모니터링 작업을 수행할 사람
- 문제 발생 시 알려야 할 대상

AWS 는 DataSync를 모니터링하기 위한 다양한 서비스와 도구를 제공합니다. 이러한 도구 중에는 모니터링을 자동으로 수행하도록 구성할 수 있으며, 수동 작업이 필요한 경우도 있습니다. 모니터링 작업은 최대한 자동화하는 것이 좋습니다.

주제

- 데이터 전송 성능 카운터 이해
- Amazon CloudWatch 지표를 사용한 데이터 전송 모니터링
- 작업 보고서로 데이터 전송 모니터링
- Amazon CloudWatch Logs를 사용한 데이터 전송 모니터링
- 를 사용하여 AWS DataSync API 호출 로깅 AWS CloudTrail
- Amazon EventBridge을 사용한 이벤트 모니터링
- 수동 도구를 AWS DataSync 사용한 모니터링

데이터 전송 성능 카운터 이해

작업을 시작하면는 데이터 전송의 성능과 진행 상황을 추적하는 데 도움이 되는 카운터를 AWS DataSync 제공합니다.

다음 정보를 사용하여 각 카운터가 무엇을 나타내는지 확인합니다. DataSync 콘솔 또는 DescribeTaskExecution 응답에서 이러한 카운터를 확인할 수 있습니다. 일부 카운터는 모든 작업 모드에서 사용할 수는 없습니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
–	`BytesWritten`	확장, 기본	DataSync가 실제로 대상 위치에 기록한 논리적 바이트 수입니다.
데이터 처리량	–	확장, 기본	DataSync가 대상 위치에 논리적 바이트를 기록하는 속도입니다. DescribeTaskExecution을 사용하는 경우 이 카운터를 계산하는 방법은 작업 모드에 따라 달라집니다. • 확장 모드: `TotalDuration` 으로 `BytesWritten` 나누기 • 기본 모드: `TransferDuration` 으로 `BytesWritten` 나누기
전송된 데이터	`BytesTransferred`	확장, 기본	DataSync가 압축(가능한 경우) 전에 네트워크에 전송하는 바이트 수입니다.

콘솔	DescribeTaskExecution	작업 모드 지원	설명
			네트워크를 통해 전송된 바이트 수는 네트워크 처리량(콘솔 내) 또는 BytesCompressed (DescribeTaskExecution) 카운터를 참조하세요.
대상에서 삭제됨	FilesDeleted	기본	DataSync가 실제로 대상 위치에서 삭제한 파일, 객체, 디렉터리 수입니다. 소스에 없는 데이터를 대상에서 삭제하도록 작업을 구성하지 않은 경우: • 대상에서 삭제됨이 콘솔에 표시되지 않습니다. • FilesDeleted 은 항상 0 값을 표시합니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
대상에서 삭제됨	`FilesDeleted` , `FoldersDeleted`	확장	DataSync가 대상 위치에서 실제로 삭제하는 파일 또는 객체 및 디렉터리의 수입니다. 소스에 없는 데이터를 대상에서 삭제하도록 작업을 구성하지 않은 경우: • 대상에서 삭제됨이 콘솔에 표시되지 않습니다. • `FilesDeleted` 및는 `FoldersDeleted` 항상 값을 표시합니다`0`.
–	`EstimatedBytesToTransfer`	확장, 기본	DataSync가 대상 위치에 기록할 것으로 예상되는 논리적 바이트 수입니다.
–	`EstimatedFilesToDelete`	기본	DataSync가 대상 위치에서 삭제할 것으로 예상되는 파일, 객체, 디렉터리 수입니다. 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성하지 않는 경우 값은 항상 `0`입니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
–	`EstimatedFilesToDelete` , `EstimatedFoldersToDelete`	확장	DataSync가 대상 위치에서 삭제할 것으로 예상되는 파일 또는 객체 및 디렉터리의 수입니다. 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성하지 않는 경우 값은 항상 `0`입니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명

–	`EstimatedFilesToTransfer`	기본	네트워크를 통해 DataSync가 전송할 것으로 예상되는 파일, 객체, 디렉터리 수입니다. 이 값은 DataSync가 전송을 준비하는 동안 계산됩니다.
			
			계산 방법은 주로 사용 중인 전송 모드에 따라 달라집니다.
			
			• 전송 모드가 변경된 데이터만 전송하도록 설정된 경우: 계산은 소스 및 대상 위치의 콘텐츠를 비교하여 이를 바탕으로 어떤 차이점을 전송해야 할지 결정합니다. 차이점은 다음과 같습니다.
			  • 소스 위치에 추가되거나 수정된 모든 항목입니다.
			  • 초기 전송 후 소스 및 대상 모두에 존재하며 대상에서 수정된 항목(작업이 대상 데이터를 덮어쓰지 않도록 구성된 경우는 제외)입니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
			• DataSync가 삭제할 것으로 예상되는 항목 수입니다(대상의 데이터를 삭제하도록 작업을 구성하는 경우). • 전송 모드가 모든 데이터를 전송하도록 설정된 경우: 계산은 DataSync가 소스 위치에서 찾는 항목만을 기준으로 수행됩니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명

–	`EstimatedFilesToTransfer`, `EstimatedFoldersToTransfer`	확장	DataSync가 네트워크를 통해 전송할 것으로 예상되는 파일 또는 객체 및 디렉터리의 수입니다. 이 값은 DataSync가 전송을 준비하는 동안 계산됩니다.
			
			계산 방법은 주로 사용 중인 전송 모드에 따라 달라집니다.
			
			• 전송 모드가 변경된 데이터만 전송하도록 설정된 경우: 계산은 소스 및 대상 위치의 콘텐츠를 비교하여 이를 바탕으로 어떤 차이점을 전송해야 할지 결정합니다. 차이점은 다음과 같습니다.
			  • 소스 위치에 추가되거나 수정된 모든 항목입니다.
			  • 초기 전송 후 소스 및 대상 모두에 존재하며 대상에서 수정된 항목(작업이 대상 데이터를 덮어쓰지 않도록 구성된 경우는 제외)입니다.

콘솔	DescribeTaskExecution	작업 모드 지원	설명
			• 전송 모드가 모든 데이터를 전송하도록 설정된 경우: 계산은 DataSync가 소스 위치에서 찾는 항목만을 기준으로 수행됩니다.
파일 처리량	–	확장, 기본	DataSync가 네트워크를 통해 파일, 객체, 디렉터리를 전송하는 속도입니다. DescribeTaskExecution을 사용하는 경우 이 카운터를 계산하는 방법은 작업 모드에 따라 달라집니다. • 확장 모드: `TotalDuration` 으로 `FilesTransferred` 나누기 • 기본 모드: `TransferDuration` 으로 `FilesTransferred` 나누기

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
–	`FilesFailed` , `FoldersFailed`	확장	작업 실행 중에 DataSync가 준비, 전송, 확인 및 삭제하지 못하는 파일 또는 객체 및 디렉터리의 수입니다. 실패한 항목이 있는 경우 대상 콘솔 카운터에서 준비됨, 전송됨, 건너뜀, 삭제됨 상태와 함께 각 항목을 확인할 수 있습니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
소스에 나열됨	`FilesListed.AtSource` , `FoldersListed.AtSource`	확장	DataSync가 소스 위치에서 찾는 파일 또는 객체 및 디렉터리의 수입니다. • 매니페스트를 사용하면 DataSync는 매니페스트에 있는 항목(소스 위치의 모든 항목 아님)만 나열합니다. • 포함 필터를 사용하면 DataSync는 소스 위치에서 필터와 일치하는 항목만 나열합니다. • 제외 필터를 사용하면 DataSync는 필터를 적용하기 전에 소스 위치에 있는 모든 항목을 나열합니다.
–	`FilesListed.AtDestinationForDelete` , `FoldersListed.AtDestinationForDelete`	확장	DataSync가 대상 위치에서 찾는 파일 또는 객체 및 디렉터리의 수입니다. 이 카운터는 대상에서 소스에 없는 데이터를 삭제하도록 작업을 구성한 경우에만 적용됩니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
네트워크 처리량*	`BytesCompressed`	확장, 기본	DataSync가 압축(가능한 경우) 후 네트워크를 통해 전송하는 물리적 바이트 수입니다. 데이터를 압축할 수 없는 경우를 제외하고, 이 수는 일반적으로 전송된 데이터(콘솔 내) 또는 `BytesTransferred` (DescribeTaskExecution)보다 적습니다. * Enhanced 모드의 경우 콘솔에 네트워크 처리량이 표시되지 않습니다.
압축 비율	–	확장, 기본	DataSync가 네트워크를 통해 전송하기 전에 압축한 전송 데이터의 비율입니다. DescribeTaskExecution을 사용하는 경우 `1 - BytesCompressed / BytesWritten` 를 사용하여 이 카운터를 계산할 수 있습니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
준비됨	`FilesPrepared` , `FoldersPrepared`	확장	소스 위치와 대상 위치를 비교한 후 DataSync가 전송을 시도할 파일 또는 객체 및 디렉터리의 수입니다. 또한 콘솔에서 이 카운터는 DataSync가 준비 중에 건너뛴 객체 수를 표시할 수 있습니다. 자세한 내용은 DataSync가 데이터 전송을 준비하는 방법 단원을 참조하십시오. 모든 데이터를 전송하도록 작업을 구성하는 경우 이 카운터를 사용할 수 없습니다. 이 시나리오에서 DataSync는 위치 간의 차이를 비교하지 않고 소스의 모든 데이터를 대상으로 복사합니다.

콘솔	`DescribeTaskExecution`	작업 모드 지원	설명
처리 속도	–	확장, 기본	DataSync가 소스 위치에서 파일, 객체, 디렉터리를 읽는 속도입니다. 처리 속도는 여러 CloudWatch 지표를 기반으로 합니다. 정확한 지표는 사용 중인 작업 모드에 따라 달라집니다. 확장 모드: • `FilesListedSource` • `FilesPrepared` • `FilesTransferred` • `FilesVerified` 기본 모드: • `FilesPreparedSource` • `FilesPreparedDestination` • `FilesTransferred` • `FilesVerifiedSource`

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
			• FilesVerifiedDestination
나머지	–	기본	네트워크를 통해 DataSync가 전송할 것으로 예상되는 파일, 객체, 디렉터리 수입니다. DescribeTaskExecution을 사용하는 경우 EstimatedFilesToTransfer 에서 FilesTransferred 을 뺀 값으로 이 카운터를 계산할 수 있습니다.
건너뜀*	FilesSkipped	기본	DataSync가 전송 중에 건너뛴 파일, 객체, 디렉터리의 수입니다.
–	FilesSkipped , FoldersSkipped	확장	전송 중에 DataSync가 건너뛰는 파일 또는 객체 및 디렉터리의 수입니다. 건너뛴 항목은 변경된 데이터만 전송할 때 준비된 카운터에 포함되고, 모든 데이터를 전송할 때 전송된 카운터에 포함됩니다.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
전송됨	FilesTransferred	기본	네트워크를 통해 DataSync가 전송하는 파일, 객체, 디렉터리 수입니다. 이 값은 작업 실행 중 소스에서 무언가를 읽어 네트워크를 통해 전송할 때 주기적으로 업데이트됩니다. DataSync가 무언가를 전송하지 못하면 이 값은 EstimatedFilesToTransfer 또는 보다 작을 수 있습니다EstimatedFoldersToTransfer . 경우에 따라이 값이 EstimatedFilesToTransfer 또는 보다 클 수도 있습니다EstimatedFoldersToTransfer . 이 카운터는 일부 위치 유형에서 구현 방식에 따라 달라지므로 이를 정확한 지표로서 사용하거나 작업 실행을 모니터

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
			링하는 데 사용하지 마세요.

콘솔	**DescribeTaskExecution**	작업 모드 지원	설명
전송됨	`FilesTransferred` , `FoldersTransferred`	확장	DataSync가 네트워크를 통해 전송하는 파일 또는 객체 및 디렉터리의 수입니다. 이 값은 작업 실행 중 소스에서 무언가를 읽어 네트워크를 통해 전송할 때 주기적으로 업데이트됩니다. DataSync가 무언가를 전송하지 못하면 이 값은 `EstimatedFilesToTransfer` 또는 보다 작을 수 있습니다`EstimatedFoldersToTransfer` . 경우에 따라이 값이 `EstimatedFilesToTransfer` 또는 보다 클 수도 있습니다`EstimatedFoldersToTransfer` . 이 카운터는 일부 위치 유형에서 구현 방식에 따라 달라지므로 이를 정확한 지표로서 사용하거나 작업 실행을 모니터

콘솔	DescribeTaskExecution	작업 모드 지원	설명
			링하는 데 사용하지 마세요.
확인됨	FilesVerified	기본	DataSync가 전송 중에 확인한 파일, 객체, 디렉터리의 수입니다. 전송된 데이터만 확인하도록 작업을 구성하면 DataSync는 일부 상황에서 디렉터리를 확인하지 않거나 전송에 실패한 파일, 객체를 확인하지 않습니다.
확인됨	FilesVerified , FoldersVerified	확장	DataSync가 전송 중에 확인하는 파일 또는 객체 및 디렉터리의 수입니다.

Amazon CloudWatch 지표를 사용한 데이터 전송 모니터링

Amazon CloudWatch는 DataSync 전송 성능을 추적하고 전송 작업 관련 문제를 해결하기 위한 지표를 제공합니다.

Amazon CloudWatch 지표를 사용하여 AWS DataSync 전송 성능을 모니터링할 수 있습니다. DataSync 지표는 CloudWatch에 5분 간격으로 자동 전송됩니다(로깅 구성 방법에 관계없이). 해당 지표는 15개월 동안 보존됩니다.

DataSync에 대한 CloudWatch 지표를 보려면 다음 도구를 사용할 수 있습니다.

- CloudWatch 콘솔
- 클라우드워치 CLI
- CloudWatch API
- DataSync 콘솔(작업 실행의 세부 정보 페이지)

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

DataSync를 위한 CloudWatch 지표

DataSync 지표는 aws/datasync네임스페이스를 사용하며, 다음 차원에 대한 지표를 제공합니다:

- AgentId - 에이전트의 고유 ID입니다(작업에서 에이전트를 사용하는 경우).
- TaskId – 과업의 고유 ID. `task-01234567890abcdef` 형식을 사용합니다.

aws/datasync 네임스페이스에는 다음과 같은 지표가 포함됩니다. 일부 지표는 모든 작업 모드에서 사용할 수는 없습니다.

CloudWatch 지표	작업 모드 지원	설명
BytesCompressed	기본	DataSync가 압축(가능한 경우) 후 네트워크를 통해 전송하는 물리적 바이트 수입니다. 일반적으로 이 수치는 데이터를 압축할 수 없는 경우를 제외하고 BytesTransferred 보다 작습니다. 단위: 바이트
BytesPreparedDestination	기본	DataSync가 대상 위치에서 준비한 논리적 바이트 수입니다. 단위: 바이트
BytesPreparedSource	기본	DataSync가 소스 위치에서 준비한 논리적 바이트 수입니다. 단위: 바이트
BytesTransferred	기본	DataSync가 압축(가능한 경우) 전에 네트워크에 전송하는 바이트 수입니다. 네트워크를 통해 전송된 바이트 수에 대한 내용은 BytesCompressed 지표를 참조하세요. 단위: 바이트
BytesVerifiedDestination	기본	DataSync가 대상 위치에서 확인한 논리적 바이트 수입니다.

CloudWatch 지표	작업 모드 지원	설명
		단위: 바이트
BytesVerifiedSource	기본	DataSync가 소스 위치에서 확인한 논리적 바이트 수입니다. 단위: 바이트
BytesWritten	확장, 기본	DataSync가 대상 위치에 기록한 논리적 바이트 수입니다. 단위: 바이트
FilesDeleted	확장, 기본	DataSync가 대상 위치에서 삭제한 파일, 객체, 디렉터리 수입니다. 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성하지 않는 경우 값은 항상 0입니다. 단위: 개
FilesListedSource	확장	DataSync가 소스 위치에서 찾는 객체 수입니다. 단위: 개
FilesPrepared	확장	DataSync가 소스 위치와 대상 위치를 비교한 후 전송을 시도할 객체 수입니다. 자세한 내용은 DataSync가 데이터 전송을 준비하는 방법 섹션을 참조하세요. 모든 데이터를 전송하도록 작업을 구성하는 경우 이 지표를 적용할 수 없습니다. 이 시나리오에서 DataSync는 위치 간의 차이를 비교하지 않고 소스의 모든 데이터를 대상으로 복사합니다. 단위: 개
FilesPreparedDestination	기본	DataSync가 대상 위치에 준비한 파일, 객체, 디렉터리의 수입니다. 단위: 개

CloudWatch 지표	작업 모드 지원	설명
`FilesPreparedSource`	기본	DataSync가 소스 위치에 준비한 파일, 객체, 디렉터리의 수입니다. 단위: 개
`FilesSkipped`	기본	DataSync가 전송 중에 건너뛴 파일, 객체, 디렉터리의 수입니다. 단위: 개
`FilesTransferred`	확장, 기본	네트워크를 통해 DataSync가 전송하는 파일, 객체, 디렉터리 수입니다. 이 값은 작업 실행 중 소스에서 무언가를 읽어 네트워크를 통해 전송할 때 주기적으로 업데이트됩니다. **Note** DataSync가 무언가를 전송하지 못하는 경우 이 값은 DescribeTaskExecution 응답의 `EstimatedFilesToTransfer` 보다 작을 수 있습니다. 경우에 따라 이 값은 `EstimatedFilesToTransfer` 보다 클 수도 있습니다. 이 지표는 일부 위치 유형에서 구현과 관련이 있으므로 이를 올바른 전송 지표로서 사용하거나 혹은 작업 실행을 모니터링하는 데 사용하지 마십시오. 단위: 개
`FilesVerified`	확장	DataSync가 전송 중에 확인한 객체 수입니다. 단위: 개
`FilesVerifiedDestination`	기본	DataSync가 대상 위치에서 확인한 파일, 객체, 디렉터리의 수입니다. 단위: 개

CloudWatch 지표	작업 모드 지원	설명
`FilesVerifiedSource`	기본	DataSync가 소스 위치에서 확인한 파일, 객체, 디렉터리의 수입니다. 단위: 개

작업 보고서로 데이터 전송 모니터링

작업 보고서는 작업 실행 중에 AWS DataSync 의 전송, 건너뛰기, 확인, 삭제 시도에 대한 자세한 정보를 제공합니다. 자세한 내용은 DataSync가 파일, 객체, 디렉터리를 전송하는 방법 단원을 참조하십시오.

작업 보고서는 JSON 형식으로 생성됩니다. 보고서에서 세부 수준을 사용자 지정할 수 있습니다.

- 요약 전용 작업 보고서는 전송된 파일 수, DataSync가 해당 파일의 데이터 무결성을 확인할 수 있는지 여부 등 작업 실행에 필요한 세부 정보를 제공합니다.
- 표준 작업 보고서에는 DataSync가 전송, 건너뛰기, 확인 및 삭제하려고 시도하는 각 파일, 객체 또는 폴더를 나열하는 요약 및 세부 보고서가 포함됩니다. 표준 작업 보고서를 사용하면 작업 실행의 오류 또는 성공 및 오류만 표시하도록 보고서 수준을 지정할 수도 있습니다.

사용 사례

다음은 작업 보고서가 데이터 전송을 모니터링하고 감사하는 데 도움이 될 수 있는 몇 가지 상황입니다.

- 수백만 개의 파일을 마이그레이션할 때 DataSync에 전송 문제가 있는 파일을 빠르게 식별합니다.
- 파일의 관리 연속성 프로세스를 확인합니다.

요약 전용 작업 보고서

작업 실행 요약만 제공하는 보고서에는 다음과 같은 세부 정보가 포함됩니다.

- 작업 실행을 실행 AWS 계정 한
- 소스 및 대상 위치
- 건너뛰고, 전송하고, 확인하고, 삭제한 파일, 객체, 폴더의 전체 수

- 전송된 총 바이트(논리적 및 물리적)
- 작업 실행이 완료되었거나 취소되었거나 오류가 발생한 경우
- 시작 및 종료 시간(총 전송 시간 포함)
- 작업 설정(예: 대역폭 제한, 데이터 무결성 확인, DataSync 전송을 위한 기타 옵션)

표준 작업 보고서

표준 작업 보고서에는 작업 실행에 대한 요약과 DataSync가 전송, 건너뛰기, 확인 및 삭제하려고 시도하는 것에 대한 세부 보고서가 포함됩니다.

주제

- 보고서 수준
- 전송된 보고서
- 건너뛴 보고서
- 확인된 보고서
- 삭제된 보고서

보고서 수준

표준 작업 보고서를 사용하면 다음 보고서 수준 중 하나를 선택할 수 있습니다.

- 오류만
- 성공 및 오류(기본적으로 작업 실행 중에 발생한 모든 일의 목록)

예를 들어 DataSync가 전송 중에 성공적으로 건너뛰었던 파일과 그렇지 않은 파일을 확인할 수 있습니다.g DataSync에서 건너뛰는 데 성공한 파일은 대상 위치에 이미 존재하므로 DataSync에서 의도적으로 제외하려는 파일일 수 있습니다. 그러나 인스턴스에 대한 건너뛰는 오류는 DataSync에 파일을 읽을 수 있는 올바른 권한이 없다는 것을 나타낼 수 있습니다.

전송된 보고서

DataSync가 작업 실행 중에 전송을 시도한 파일, 객체 및 디렉터리 목록입니다. 전송된 보고서에는 다음과 같은 세부 정보가 포함됩니다.

- 전송된 데이터의 경로
- 전송된 내용(콘텐츠, 메타데이터 또는 둘 다)

- 데이터 유형, 컨텐츠 크기(객체 및 파일만 해당) 등을 포함하는 메타데이터
- 항목이 전송된 시간
- 객체 버전(대상이 버전 관리가 사용 설정된 Amazon S3 버킷인 경우)
- 대상에서 무언가를 덮어쓴 경우
- 항목이 성공적으로 전송되었는지 여부

> **Note**
>
> S3 버킷 간에 데이터를 이동할 때 소스 위치에 지정한 접두사가 보고서(또는 Amazon CloudWatch Logs)에 표시될 수 있습니다. 이는 해당 접두사가 대상 위치에 객체로 존재하지 않더라도 마찬가지입니다. (DataSync 콘솔에서 이 접두사가 건너뛰었거나 검증된 데이터로 표시되는 것을 확인할 수도 있습니다.)

건너뛴 보고서

DataSync가 소스 위치에서 발견했지만 전송을 시도하지 않은 파일, 객체, 디렉터리의 목록입니다. DataSync가 데이터를 건너뛰는 이유는 작업 구성 방법과 스토리지 시스템 권한 등 여러 요인에 따라 달라질 수 있습니다. 여기 몇 가지 예가 있습니다:

- 소스 위치 및 대상 위치의 파일이 이미 있습니다. 소스의 파일은 이전 작업 실행 이후 수정되지 않았습니다. DataSync는 변경된 데이터만 전송하므로 다음 번에 작업을 실행할 때 해당 파일을 전송하지 않습니다.
- 두 위치에 모두 존재하는 객체가 소스에서 변경됩니다. 태스크가 대상의 데이터를 덮어쓰지 않기 때문에 태스크를 실행하면 DataSync는 대상에서 이 객체를 건너뜁니다.
- DataSync는 아카이브 스토리지 클래스를 사용 중이며 복원되지 않은 소스 내 객체를 건너뜁니다. DataSync가 읽을 수 있도록 아카이브된 객체를 복원해야 합니다.
- DataSync가 소스 위치에서 파일, 객체, 디렉터리를 읽을 수 없으므로 이를 건너뜁니다. 이런 일이 예상치 못하게 발생한 경우, 스토리지의 액세스 권한을 확인하고 DataSync가 건너뛴 항목을 읽을 수 있는지 확인하세요.

건너뛴 보고서에는 다음과 같은 세부 정보가 포함됩니다.

- 건너뛰는 데이터의 경로
- 항목을 건너뛰었던 시간

- 항목을 건너뛰게 된 이유
- 항목을 성공적으로 건너뛰었는지 여부

> **Note**
>
> 건너뛴 보고서에 성공 및 오류가 포함되고, 변경된 데이터만 전송하도록 작업을 구성하고, 소스 데이터가 대상에 이미 있는 경우 건너뛴 보고서가 클 수 있습니다.

확인된 보고서

DataSync가 작업 실행 중에 무결성을 확인하려고 시도한 파일, 객체 및 디렉터리 목록입니다. 검증된 데이터 보고서에는 다음과 같은 세부 정보가 포함됩니다.

- 검증된 데이터의 경로
- 항목이 검증된 시간
- 확인 오류 이유(있는 경우)
- 소스 및 대상 SHA256 체크섬(파일만 해당)
- 항목이 성공적으로 확인되었는지 여부

확인된 보고서에 관한 다음 사항에 유의하세요.

- 전송된 데이터만 확인하도록 작업을 구성하면 DataSync는 일부 상황에서 디렉터리를 확인하지 않거나 전송에 실패한 파일, 객체를 확인하지 않습니다. 어느 경우든 DataSync는 검증되지 않은 데이터를 이 보고서에 포함하지 않습니다.
- 확장 모드를 사용하는 경우 대용량 객체 전송 시 확인 작업에 평소보다 오랜 시간이 걸릴 수 있습니다.

삭제된 보고서

작업 실행 중에 삭제된 파일, 디렉터리 및 객체의 목록입니다. 이는 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성한 경우에만 DataSync가 이 보고서를 생성합니다. 삭제된 데이터 보고서에는 다음과 같은 세부 정보가 포함됩니다.

- 삭제된 데이터 경로
- 항목이 성공적으로 삭제되었는지 여부

- 항목을 삭제한 시간

작업 보고서 예제

작업 보고서의 세부 수준은 사용자에게 달려 있습니다. 다음 구성으로 전송된 데이터 보고서의 몇 가지 예제입니다.

- 보고서 유형 - 표준
- 보고서 수준 - 성공 및 오류

> **Note**
>
> 보고서는 타임스탬프 형식으로 ISO-8601 표준을 사용합니다. 시간은 UTC 기준이며 나노초 단위로 측정됩니다. 이 동작은 다른 작업 보고서 지표의 측정 방식과 다릅니다. 예를 들어, `TransferDuration` 및 `VerifyDuration`과 같은 작업 실행 세부 정보는 밀리초 단위로 측정됩니다.

확장 모드 작업 보고서는 기본 모드 작업 보고서와 약간 다른 스키마를 사용합니다. 다음 예시는 사용하는 작업 모드에 따라 보고서에서 예상되는 사항을 파악하는 데 도움이 될 수 있습니다.

전송 데이터 성공 상태 보고서 예시

다음 보고서는 `object1.txt`라는 객체의 성공적인 전송을 보여줍니다.

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"
    }]
}
```

전송 데이터 오류 상태 보고서 예시

다음 보고서는 DataSync가 `object1.txt`라는 객체를 전송할 수 없는 경우의 예를 제공합니다.

Enhanced mode

이 보고서는 `object1.txt` 권한 문제로 인해 DataSync가 AWS KMS 라는 객체에 액세스할 수 없음을 보여줍니다. (이러한 오류가 발생하면 서버측 암호화를 사용하여 S3 버킷에 액세스 섹션을 참조하세요.)

```
{
    "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

이 보고서는 `object1.txt`라는 객체가 S3 버킷 권한 문제로 인해 전송되지 않았음을 보여줍니다. (이러한 오류가 발생하면 DataSync에 S3 버킷 액세스 권한 제공 섹션을 참조하세요.)

```
{
    "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
    }]
}
```

제한 사항

- 개별 작업 보고서는 5MB를 초과할 수 없습니다. 많은 파일을 복사하는 경우 작업 보고서가 여러 보고서로 분할될 수 있습니다.
- 작업 보고서를 생성할 경우 데이터 전송 성능에 영향을 미칠 수 있는 상황이 있습니다. 예를 들어 네트워크 연결 지연 시간이 길고 전송 중인 파일이 작거나 메타데이터 변경 사항만 복사하는 경우 이 문제가 발생할 수 있습니다.

DataSync 작업 보고서 생성

AWS DataSync 작업 보고서는 작업 실행 요약 또는 DataSync가 전송, 건너뛰기, 확인 및 삭제하려고 시도하는 항목에 대한 세부 보고서 세트일 수 있습니다.

사전 조건

작업 보고서를 생성하려면 먼저 다음 작업을 수행해야 합니다.

주제

- 작업 보고서를 위한 S3 버킷 생성
- DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용

작업 보고서를 위한 S3 버킷 생성

S3 버킷이 아직 없는 경우에 DataSync가 작업 보고서를 업로드할 수 있는 S3 버킷을 생성합니다. 보고서는 S3 표준 스토리지 클래스에 저장됩니다.

이 버킷에는 다음 사항을 권장합니다.

- 데이터를 S3 버킷으로 전송할 계획이라면 삭제된 파일 보관 옵션을 비활성화한 경우 작업 보고서에 동일한 버킷을 사용하지 마세요. 그렇지 않으면 DataSync는 작업을 실행할 때마다 이전 작업 보고서를 모두 삭제합니다. 해당 보고서는 소스 위치에 존재하지 않기 때문입니다.
- 복잡한 액세스 권한 설정을 방지하려면 작업 보고서 버킷이 DataSync 전송 작업과 동일한 AWS 계정 및 리전에 있어야 합니다.

DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용

DataSync가 작업 보고서를 S3 버킷에 업로드하도록 허용하는 AWS Identity and Access Management (IAM) 역할을 구성해야 합니다.

DataSync 콘솔에서 대부분의 경우 작업 보고서를 버킷에 업로드할 권한이 자동으로 포함되는 IAM 역할을 생성할 수 있습니다. 이 자동 생성된 역할은 최소 권한 관점에서 볼 때 요구 사항을 충족하지 못할 수 있다는 점에 유의하세요. 버킷이 고객 관리형 AWS Key Management Service (AWS KMS) 키(SSE-KMS)로 암호화된 경우에도이 역할은 작동하지 않습니다. 이 경우 역할이 최소한 다음 작업을 수행하기만 하면 역할을 수동으로 만들 수 있습니다.

- 역할의 신뢰할 수 있는 개체에서 교차 서비스 혼동된 대리자 문제를 방지합니다.

  다음 예는 DataSync에서 `aws:SourceArn`및 `aws:SourceAccount`전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다.

  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:*"
                }
            }
        }
    ]
}
```

- DataSync가 S3 버킷에 작업 보고서를 업로드할 수 있도록 허용합니다.

  다음 예제는 버킷의 특정 접두사(`reports/`)에 대한 `s3:PutObject`작업만 포함하여 이를 수행합니다.

  JSON

```
{
        "Version":"2012-10-17",
        "Statement": [{
            "Action": [
                "s3:PutObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::your-task-reports-bucket/reports/*"
        }]
}
```

- S3 버킷이 고객 관리형 SSE-KMS 키로 암호화된 경우 키 정책에는 DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할이 포함되어야 합니다.

  자세한 설명은 서버측 암호화를 사용하여 S3 버킷에 액세스섹션을 참조하세요.

요약 전용 작업 보고서 생성

DataSync 작업을 생성하거나, 작업을 시작하거나, 작업을 업데이트할 때만 요약이 포함된 작업 보고서를 구성할 수 있습니다.

다음 단계에서는 작업을 생성할 때 요약 전용 작업 보고서를 구성하는 방법을 보여줍니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 작업 보고서 섹션까지 아래로 스크롤합니다. 보고서 유형에서는 요약만을 선택합니다.
5. 보고서용 S3 버킷의 경우, DataSync가 작업 보고서를 업로드할 S3 버킷을 선택합니다.

   > **Tip**
   >
   > 데이터를 S3 버킷으로 전송할 계획이라면 삭제된 파일 보관 옵션을 비활성화한 경우 작업 보고서에 동일한 버킷을 사용하지 마세요. 그렇지 않으면 DataSync는 작업을 실행할 때마다 이전 작업 보고서를 모두 삭제합니다. 해당 보고서는 소스 위치에 존재하지 않기 때문입니다.
6. 폴더에는 DataSync가 보고서를 S3 버킷에 업로드할 때 작업 보고서에 사용할 접두사를 입력합니다(예:**`reports/`**).

   접두사 끝에는 적절한 구분 문자를 포함해야 합니다. 이 문자는 일반적으로 전방향 슬래시(/)입니다. 자세한 내용은 Amazon S3 사용 설명서의 접두사를 사용하여 객체 구성하기를 참조하세요.
7. IAM 역할에 대해 다음 중 하나를 수행합니다.

   - 자동 생성을 선택하여 DataSync가 S3 버킷에 액세스하는 데 필요한 권한을 가진 IAM 역할을 자동으로 생성하도록 합니다.

     이전에 DataSync에서 이 S3 버킷에 대한 IAM 역할을 만든 경우, 해당 역할이 기본적으로 선택됩니다.
   - 생성한 사용자 지정 IAM 역할을 선택합니다.

     경우에 따라 역할을 직접 생성해야 할 수도 있습니다. 자세한 설명은 DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용섹션을 참조하세요.

     > **Important**
     >
     > S3 버킷이 고객 관리형 SSE-KMS 키로 암호화된 경우 키 정책에는 DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할이 포함되어야 합니다.

자세한 설명은 서버측 암호화를 사용하여 S3 버킷에 액세스섹션을 참조하세요.

8. 작업 생성을 완료한 다음 작업을 시작하여 데이터 전송을 시작합니다.

전송이 완료되면 작업 보고서를 볼 수 있습니다.

사용 AWS CLI

1. 다음 `create-task` AWS Command Line Interface (AWS CLI) 명령을 복사합니다.

```
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. `--source-location-arn`파라미터에는 전송 시 소스 위치의 Amazon 리소스 이름(ARN)을 지정합니다. *us-east-1*를 적절한 로 AWS 리전바꾸고,를 적절한 AWS 계정 숫자*123456789012*로 바꾸고,를 적절한 소스 위치 ID*12345678abcdefgh*로 바꿉니다.
3. `--destination-location-arn` 파라미터에 대해서 전송 대상 위치의 ARN을 지정합니다. *us-east-1*를 적절한 로 AWS 리전바꾸고, *123456789012*를 적절한 AWS 계정 번호로 바꾸고,를 적절한 대상 위치 ID*abcdefgh12345678*로 바꿉니다.
4. `--task-report-config` 파라미터에 관하여 다음을 수행합니다.

   - Subdirectory- *reports/*를 DataSync에서 작업 보고서를 업로드할 S3 버킷의 접두사로 바꾸세요.

     접두사 끝에는 적절한 구분 문자를 포함해야 합니다. 이 문자는 일반적으로 전방향 슬래시(/)입니다. 자세한 내용은 Amazon S3 사용 설명서의 접두사를 사용하여 객체 구성하기를 참조하세요.

- `S3BucketArn`- 작업 보고서를 업로드하려는 S3 버킷의 ARN을 지정합니다.

  > **Tip**
  >
  > 데이터를 S3 버킷으로 전송할 계획이라면 삭제된 파일 보관 옵션을 비활성화한 경우 작업 보고서에 동일한 버킷을 사용하지 마세요. 그렇지 않으면 DataSync는 작업을 실행할 때마다 이전 작업 보고서를 모두 삭제합니다. 해당 보고서는 소스 위치에 존재하지 않기 때문입니다.

- `BucketAccessRoleArn`- DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용하는 IAM 역할을 지정합니다.

  자세한 설명은 DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용섹션을 참조하세요.

  > **Important**
  >
  > S3 버킷이 고객 관리형 SSE-KMS 키로 암호화된 경우 키 정책에는 DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할이 포함되어야 합니다.
  > 자세한 설명은 서버측 암호화를 사용하여 S3 버킷에 액세스섹션을 참조하세요.

- `OutputType` - `SUMMARY_ONLY`을(를) 지정합니다.

  자세한 설명은 요약 전용 작업 보고서섹션을 참조하세요.

5. `create-task` 명령을 실행하여 작업을 생성합니다.

   생성한 작업의 ARN을 보여주는 다음과 같은 응답을 받게 됩니다. `start-task-execution`명령을 실행하려면 이 ARN이 필요합니다.

   ```
   {
       "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
   }
   ```

6. 다음 `start-task-execution`명령을 복사합니다.

   ```
   aws datasync-task-report start-task-execution \
     --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
   ```

7. `--task-arn` 파라미터에는 시작하려는 작업의 ARN을 지정합니다. `create-task`명령을 실행하여 받은 ARN을 사용합니다.

8. `start-task-execution` 명령을 실행합니다.

전송이 완료되면 작업 보고서를 볼 수 있습니다.

표준 태스크 보고서 생성

DataSync 작업을 만들거나, 작업을 시작하거나, 작업을 업데이트할 때 표준 작업 보고서를 구성할 수 있습니다.

다음 단계에서는 작업을 생성할 때 표준 작업 보고서를 구성하는 방법을 보여줍니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 작업 보고서 섹션까지 아래로 스크롤합니다. 보고서 유형에서 표준 보고서를 선택합니다.
5. Report 수준에서 다음 중 하나를 선택합니다.

   - 오류만 - 작업 보고서에는 DataSync가 전송, 건너뛰기, 확인 및 삭제를 시도한 항목과 관련된 문제만 포함됩니다.
   - 성공 및 오류 - 작업 보고서에는 DataSync가 성공적으로 전송, 건너뛰고, 검증하고, 삭제한 내용과 그렇지 않은 내용이 포함됩니다.
   - 사용자 지정 - 작업 보고서의 특정 측면에 대한 오류만 표시할지 또는 성공과 오류를 표시할지 선택할 수 있습니다.

     예를 들어 전송된 파일 목록에서는 성공 및 오류를 선택하고 나머지 보고서에서는 오류만 선택할 수 있습니다.
6. 객체 버전 관리를 사용하는 S3 버킷으로 전송하는 경우, 전송된 각 객체의 새 버전을 보고서에 포함하려면 Amazon S3 객체 버전을 포함시킬 것을 선택한 상태로 유지하세요.
7. 보고서용 S3 버킷의 경우, DataSync가 작업 보고서를 업로드할 S3 버킷을 선택합니다.

   > **Tip**
   >
   > 데이터를 S3 버킷으로 전송할 계획이라면 삭제된 파일 보관 옵션을 비활성화한 경우 작업 보고서에 동일한 버킷을 사용하지 마세요. 그렇지 않으면 DataSync는 작업을 실행할 때마

다 이전 작업 보고서를 모두 삭제합니다. 해당 보고서는 소스 위치에 존재하지 않기 때문입니다.

8. 폴더에는 DataSync가 보고서를 S3 버킷에 업로드할 때 작업 보고서에 사용할 접두사를 입력합니다(예:**`reports/`**). 접두사 끝에는 적절한 구분 문자를 포함해야 합니다. 이 문자는 일반적으로 전방향 슬래시(/)입니다. 자세한 내용은 Amazon S3 사용 설명서의 접두사를 사용하여 객체 구성하기를 참조하세요.
9. IAM 역할에 대해 다음 중 하나를 수행합니다.

   - 자동 생성을 선택하여 DataSync가 S3 버킷에 액세스하는 데 필요한 권한을 가진 IAM 역할을 자동으로 생성하도록 합니다.

     이전에 DataSync에서 이 S3 버킷에 대한 IAM 역할을 만든 경우, 해당 역할이 기본적으로 선택됩니다.
   - 생성한 사용자 지정 IAM 역할을 선택합니다.

     경우에 따라 역할을 직접 생성해야 할 수도 있습니다. 자세한 설명은 DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용섹션을 참조하세요.

     > **Important**
     >
     > S3 버킷이 고객 관리형 SSE-KMS 키로 암호화된 경우 키 정책에는 DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할이 포함되어야 합니다.
     > 자세한 설명은 서버측 암호화를 사용하여 S3 버킷에 액세스섹션을 참조하세요.
10. 작업 생성을 완료하고 작업을 시작하여 데이터 전송을 시작합니다.

전송이 완료되면 작업 보고서를 볼 수 있습니다.

사용 AWS CLI

1. 다음 `create-task`명령을 복사합니다.

```
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. `--source-location-arn`파라미터에는 전송 시 소스 위치의 ARN을 지정합니다. *us-east-1*를 적절한 로 AWS 리전바꾸고,를 적절한 AWS 계정 숫자*123456789012*로 바꾸고,를 적절한 소스 위치 ID*12345678abcdefgh*로 바꿉니다.
3. `--destination-location-arn` 파라미터에 대해서 전송 대상 위치의 ARN을 지정합니다. *us-east-1*를 적절한 로 AWS 리전바꾸고, *123456789012*를 적절한 AWS 계정 번호로 바꾸고, 를 적절한 대상 위치 ID*abcdefgh12345678*로 바꿉니다.
4. `--task-report-config` 파라미터에 관하여 다음을 수행합니다.

   - `Subdirectory`- *reports/*를 DataSync에서 작업 보고서를 업로드할 S3 버킷의 접두사로 바꾸세요. 접두사 끝에는 적절한 구분 문자를 포함해야 합니다. 이 문자는 일반적으로 전방향 슬래시(/)입니다. 자세한 내용은 Amazon S3 사용 설명서의 접두사를 사용하여 객체 구성하기를 참조하세요.
   - `S3BucketArn`- 작업 보고서를 업로드하려는 S3 버킷의 ARN을 지정합니다.

     > **Tip**
     >
     > 데이터를 S3 버킷으로 전송할 계획이라면 삭제된 파일 보관 옵션을 비활성화한 경우 작업 보고서에 동일한 버킷을 사용하지 마세요. 그렇지 않으면 DataSync는 작업을 실행할 때마다 이전 작업 보고서를 모두 삭제합니다. 해당 보고서는 소스 위치에 존재하지 않기 때문입니다.

   - `BucketAccessRoleArn`- DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용하는 IAM 역할을 지정합니다.

     자세한 설명은 DataSync가 S3 버킷에 작업 보고서를 업로드하도록 허용섹션을 참조하세요.

> **Important**
>
> S3 버킷이 고객 관리형 SSE-KMS 키로 암호화된 경우 키 정책에는 DataSync가 버킷에 액세스하는 데 사용하는 IAM 역할이 포함되어야 합니다.
> 자세한 설명은 서버측 암호화를 사용하여 S3 버킷에 액세스섹션을 참조하세요.

- `OutputType`- `STANDARD`보고서를 지정하세요.

  자세한 내용은 표준 작업 보고서작업 보고서 유형을 참조하십시오.

- (선택 사항) `ReportLevel`- `SUCCESSES_AND_ERRORS`보고서 내에(`ERRORS_ONLY`기본값)을(를) 원하는지 지정합니다.
- (선택 사항) `ObjectVersionIds`- 객체 버전 관리를 사용하는 S3 버킷으로 전송하는 경우, 전송된 각 객체에 대한 새 버전을 보고서에 포함시키고 싶지 않다면 `NONE`을(를) 지정하세요.

  기본적으로 이 옵션은 `INCLUDE`(으)로 설정되어 있습니다.

- (선택 사항) `Overrides`- 보고서의 특정 양상의 `ReportLevel`을 사용자 지정합니다.

  예를 들어 DataSync가 대상 위치에서 삭제하는 항목의 목록에 관하여 `SUCCESSES_AND_ERRORS`을 보고 싶지만 그 밖의 모든 항목에 관해서는 `ERRORS_ONLY`를 원할 수 있습니다. 이 예시에서는 `--task-report-config`파라미터에 다음 `Overrides`옵션을 추가합니다.

  ```
  "Overrides":{
    "Deleted":{
      "ReportLevel":"SUCCESSES_AND_ERRORS"
    }
  }
  ```

  `Overrides`을 사용하지 않는 경우, 전체 보고서에서 귀하가 지정한 `ReportLevel`를 사용합니다.

5. `create-task` 명령을 실행하여 작업을 생성합니다.

   생성한 작업의 ARN을 보여주는 다음과 같은 응답을 받게 됩니다. `start-task-execution`명령을 실행하려면 이 ARN이 필요합니다.

   ```
   {
       "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
   ```

```
}
```

6. 다음 `start-task-execution`명령을 복사합니다.

```
aws datasync-task-report start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

7. `--task-arn` 파라미터에는 실행 중인 작업의 ARN을 지정합니다. `create-task` 명령을 실행하여 받은 ARN을 사용합니다.
8. `start-task-execution` 명령을 실행합니다.

전송이 완료되면 작업 보고서를 볼 수 있습니다.

DataSync 작업 보고서 보기

DataSync는 모든 작업 실행에 대한 작업 보고서를 생성합니다. 실행이 완료되면 S3 버킷에서 관련 작업 보고서를 찾을 수 있습니다. 작업 보고서는 작업 및 실행 ID를 포함하는 접두사로 구성됩니다.

S3 버킷에서 작업 보고서를 찾는 데 도움이 되도록 다음 예제를 사용하세요.

- 요약 전용 작업 보고서 - *reports-prefix*/Summary-Reports/*task-id-folder*/*task-execution-id-folder*
- 표준 작업 보고서 - *reports-prefix*/Detailed-Reports/*task-id-folder*/*task-execution-id-folder*

작업 보고서는 JSON 형식이므로 보고서를 볼 수 있는 몇 가지 옵션이 있습니다.

- Amazon S3 Select를 사용하여 보고서를 봅니다.
- AWS Glue Amazon Athena 및 Amazon Quick과 같은 AWS 서비스를 사용하여 보고서를 시각화합니다. 작업 보고서를 시각화하는 방법에 대한 자세한 내용은 AWS 스토리지 블로그를 참조하세요.

Amazon CloudWatch Logs를 사용한 데이터 전송 모니터링

CloudWatch Logs를 사용하여 AWS DataSync 전송을 모니터링할 수 있습니다. 최소한 기본 정보(예: 전송 오류)를 기록하도록 작업을 구성하는 것이 좋습니다.

DataSync가 CloudWatch 로그 그룹에 로그를 업로드하도록 허용

DataSync 작업에 대한 로깅을 구성하려면 DataSync가 로그를 전송할 권한이 있는 CloudWatch 로그 그룹이 필요합니다. AWS Identity and Access Management (IAM) 역할을 통해이 액세스를 설정합니다. 구체적인 작동 방식은 작업 모드에 따라 달라집니다.

Enhanced mode

확장 모드에서 DataSync는 작업 로그를 `/aws/datasync`라는 로그 그룹으로 자동 전송합니다. 해당 로그 그룹이에 없는 경우 AWS 리전 DataSync는 작업을 생성할 때 IAM 서비스 연결 역할을 사용하여 사용자를 대신하여 로그 그룹을 생성합니다.

Basic mode

기본 모드를 사용하여 DataSync 작업에 대한 CloudWatch 로그 그룹을 설정하는 몇 가지 방법이 있습니다. 콘솔에서는 대부분 DataSync가 로그를 업로드하는 데 필요한 권한을 포함하는 IAM 역할을 자동으로 생성할 수 있습니다. 이 자동 생성된 역할은 최소 권한 관점에서 볼 때 요구 사항을 충족하지 못할 수 있다는 점에 유의하세요.

기존 CloudWatch 로그 그룹을 사용하거나 프로그래밍 방식으로 작업을 생성하려는 경우, 이 IAM 역할을 직접 생성해야 합니다.

다음은 이러한 권한들을 부여하는 IAM 정책의 예시입니다.

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

이 정책은 Condition문을 사용하여 지정된 계정의 DataSync 작업만 지정된 CloudWatch 로그 그룹에 액세스할 수 있도록 합니다. 혼동된 대리자 문제를 방지하려면 이러한 Condition문에 aws:SourceArn 및 aws:SourceAccount 글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다. 자세한 내용은 교차 서비스 혼동된 대리인 방지 단원을 참조하십시오.

DataSync 작업 또는 작업을 지정하려면를 작업이 AWS 리전 위치한의 리전 코드(예: us-west-2)*region*로 바꾸고를 작업이 포함된 계정의 AWS 계정 ID*account-id*로 바꿉니다. CloudWatch 로그 그룹을 지정하려면 동일한 값을 바꾸세요. 특정 로그 그룹을 대상으로 지정하도록 Resource문을 변경할 수도 있습니다. SourceArn 및 SourceAccount사용에 대한 자세한 설명은 IAM 사용자 가이드의 글로벌 조건 키를 참조하세요.

정책을 적용하려면 이 정책 설명을 로컬 컴퓨터의 파일에 저장합니다. 그런 다음 다음 AWS CLI 명령을 실행하여 리소스 정책을 적용합니다. 이 예시 명령을 사용하려면 *full-path-to-policy-file*를 정책 설명이 포함된 파일의 경로로 대체해야 합니다.

```
aws logs put-resource-policy --policy-name trust-datasync --policy-document
 file://full-path-to-policy-file
```

> **Note**
>
> DataSync 에이전트를 활성화한 동일한 AWS 계정 및 AWS 리전 를 사용하여이 명령을 실행합니다.

자세한 내용은 Amazon CloudWatch Logs 사용자 안내서를 참조하세요.

DataSync 작업에 대한 로깅 구성

DataSync 작업에 대해 일정 수준의 로깅을 구성하는 것이 좋습니다.

시작하기 전 준비 사항

DataSync에는 CloudWatch 로그 그룹에 로그를 업로드할 수 있는 권한이 필요합니다. 자세한 내용은 DataSync가 CloudWatch 로그 그룹에 로그를 업로드하도록 허용 단원을 참조하십시오.

DataSync 콘솔 사용

다음 지침에서는 작업을 생성할 때 CloudWatch 로깅을 구성하는 방법을 설명합니다. 또한 작업을 편집할 때 로깅을 구성할 수 있습니다.

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 작업을 선택하고 작업 생성을 선택합니다.
3. 태스크의 소스 및 대상 위치를 구성합니다.

   자세한 내용은 데이터를 어디로 전송할 수 있나요 AWS DataSync? 섹션을 참조하세요.
4. 설정 구성 페이지에서 작업 모드와 그 외 옵션을 선택합니다.

   다음 옵션 중 일부에 관심이 있을 수 있습니다.

   - 매니페스트 또는 필터를 사용하여 전송할 데이터를 지정합니다.
   - 파일 메타데이터를 처리하고 데이터 무결성을 확인하는 방법을 구성합니다.
5. 로그 수준에서 다음 옵션 중 하나를 선택합니다:

   - 전송 오류 같은 기초 정보 로그 - 로그에 기본 정보(예: 전송 오류)만 게시합니다.
   - 전송된 모든 객체 및 파일 로그 - DataSync가 전송하고 데이터 무결성 검사를 수행하는 모든 파일 또는 객체에 대한 로그를 게시합니다.
   - 로그 생성 안 함
6. CloudWatch 로그 그룹을 생성하거나 지정하는 데 사용하는 작업 모드에 따라 다음 중 하나를 수행합니다.

   Enhanced mode

   작업 생성을 선택하면 DataSync는 `/aws/datasync`라는 로그 그룹을 자동으로 사용(또는 생성)합니다.

Basic mode

CloudWatch 로그 그룹의 경우, 다음 중 하나를 수행하여 DataSync가 로그를 업로드할 권한이 있는 로그 그룹을 지정합니다.

- 자동 생성을 선택하여 DataSync가 로그를 업로드할 수 있는 로그 그룹을 자동으로 생성합니다.
- 현재 AWS 리전에서 기존 로그 그룹을 선택합니다.

  기존 로그 그룹을 선택하는 경우 DataSync에 해당 로그 그룹에 로그를 업로드할 권한이 있는지 확인합니다.

7. 작업 생성을 선택합니다.

작업을 시작할 준비가 되었습니다.

사용 AWS CLI

1. 다음 `create-task`명령을 복사합니다.

```
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. `--source-location-arn`에서 소스 위치의 Amazon 리소스 이름(ARN)을 지정합니다.
3. `--destination-location-arn`에서 대상 위치의 ARN을 지정합니다.

   AWS 리전 또는 계정 간에 전송하는 경우 ARN에 다른 리전 또는 계정 ID가 포함되어 있는지 확인합니다.

4. `--task-mode`에 대해 `ENHANCED` 또는 `BASIC`을 지정합니다.
5. (권장) `--name`에서 기억할 수 있는 작업의 이름을 지정합니다.
6. `LogLevel`에 대해 다음 옵션 중 하나를 지정하세요.

- `BASIC` - 기본 정보(예: 전송 오류)만 포함하여 로그를 게시합니다.
- `TRANSFER` - DataSync가 전송하는 모든 파일 또는 객체에 대한 로그를 게시하고 데이터 무결성 검사를 수행합니다.
- `NONE` - 로그를 생성하지 않습니다.

7. `-cloudwatch-log-group-arn`에 대해 CloudWatch 로그 그룹의 ARN을 지정합니다.

> **Important**
>
> `--task-mode`가 `ENHANCED`인 경우 이 옵션을 지정할 필요가 없습니다. 자세한 내용은 DataSync가 CloudWatch 로그 그룹에 로그를 업로드하도록 허용 단원을 참조하십시오.

8. `create-task` 명령을 실행합니다.

   명령이 성공하면 생성한 작업의 ARN을 보여주는 응답을 받게 됩니다. 예제:

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

작업을 시작할 준비가 되었습니다.

DataSync API 사용

다음 작업 중 하나와 함께 `CloudWatchLogGroupArn`파라미터를 사용하여 작업에 대한 CloudWatch 로깅을 구성할 수 있습니다.

- CreateTask
- UpdateTask

DataSync 작업 로그 보기

작업을 시작할 때 CloudWatch 콘솔 또는 AWS CLI (기타 옵션 중)를 사용하여 작업 실행의 로그를 볼 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용자 안내서를 참조하세요.

DataSync는 확장 모드 작업에 대한 JSON 정형 로그를 제공합니다. 기본 모드 작업은 비정형 로그를 사용합니다. 다음 예시에서는 기본 모드 로그와 비교하여 확장 모드 로그에 확인 오류가 표시되는 방법을 보여줍니다.

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
```

를 사용하여 AWS DataSync API 호출 로깅 AWS CloudTrail

AWS DataSync는 DataSync AWS 서비스 에서 사용자 AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스와 통합됩니다. CloudTrail은 DataSync를 위한 모든 API 호출을 이벤트로서 포착합니다. 포착되는 호출에는 DataSync 콘솔로부터의 호출과 DataSync API 작업향 코드 호출이 포함됩니다.

추적을 생성하면 AWS DataSync 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 이력에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 AWS DataSync에 제기된 요청, 요청을 제기한 곳의 IP 주소, 요청을 제기한 사람, 요청이 제기된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 설명은 AWS CloudTrail 사용자 가이드를 참조하세요.

CloudTrail에서의 DataSync 정보 작업

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. AWS DataSync에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 이벤트와 함께 CloudTrail AWS 서비스 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS DataSync에 대한 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 AWS 리전에 트레일이 적용됩니다. 추적은 동일한 AWS 파티션 AWS 리전 에 있는 모든의 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취 AWS 서비스 하도록 다른를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

모든 DataSync 작업은 CloudTrail에 의해 로깅됩니다. (자세한 설명은 DataSync API 참조를 참조하세요.)

예컨대, `CreateAgent`, `CreateTask`및 `ListLocations`작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부

자세한 설명은 AWS CloudTrail 사용자 가이드의 CloudTrail userIdentity요소를 참조하세요.

DataSync 로그 파일 항목의 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예는 `CreateTask`작업을 보여주는 CloudTrail 로그 항목입니다.

```
{
    "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"
}
```

Amazon EventBridge을 사용한 이벤트 모니터링

Amazon EventBridge 이벤트는 DataSync 리소스의 변경 사항을 설명합니다. 규칙을 설정하면 일치하는 이러한 이벤트를 검색하고 하나 이상의 대상 함수 또는 스트림으로 이벤트를 라우팅할 수 있습니다. 이벤트는 최선의 작업에 근거하여 발생됩니다.

DataSync 전송 이벤트

DataSync 전송에 사용할 수 있는 EventBridge 이벤트는 다음과 같습니다.

Agent state changes

이벤트	설명
Online	The agent is configured properly and ready to use. This is the normal running status for an agent.
Offline	The agent has been out of contact with the DataSync service for five minutes or longer. This can happen for a few reasons. For more information, see 에이전트가 오프라인 상태인 경우, 어떻게 해야 하나요?

Location state changes

이벤트	설명
Adding	DataSync is adding a location.
Available	The location is created and is available to use.

Task state changes

이벤트	설명
Available	The task was created and is ready to start.
Running	The task is in progress and functioning properly.

Agent state changes

Unavailable	The task isn't configured properly and can't be used. You might see this event when an agent associated with the task goes offline.
Queued	Another task is running and using the same agent. DataSync runs tasks in series (first in, first out).

Task execution state changes

이벤트	설명
Queueing	Another task execution is running and using the same DataSync agent. For more information, see 작업이 대기열에 있는 시점 파악.
Launching	DataSync is initializing the task execution. This status usually goes quickly but can take up to a few minutes.
Preparing	DataSync는 전송이 필요한 데이터를 결정합니다. 이 단계는 두 위치의 파일, 객체, 디렉터리 수와 작업 구성 방식에 따라 몇 분에서 몇 시간이 걸릴 수 있습니다. 준비는 작업에 해당하지 않을 수 있습니다. 자세한 내용은 DataSync가 데이터 전송을 준비하는 방법 단원을 참조하십시오.
Transferring	DataSync is performing the actual data transfer.
Verifying	DataSync is performing a data-integrity check at the end of the transfer.
Success	The task execution succeeded.
Cancelling	The task execution is in the process of being cancelled.

Agent state changes	
Error	The task execution failed.

수동 도구를 AWS DataSync 사용한 모니터링

콘솔 또는 명령줄에서 AWS DataSync 전송을 추적할 수 있습니다.

DataSync 콘솔을 사용하여 전송 모니터링

콘솔을 사용하여 DataSync 전송을 모니터링할 수 있습니다. 콘솔은 전송된 데이터, 데이터 및 파일 처리량, 데이터 압축과 같은 실시간 지표를 제공합니다.

DataSync 콘솔을 사용하여 전송을 모니터링하려면

1. DataSync 작업을 시작한 후 실행 세부 정보 보기를 선택합니다.
2. 전송에 대한 메트릭을 확인하세요.

를 사용하여 전송 모니터링 AWS CLI

AWS Command Line Interface ()를 사용하여 DataSync 전송을 모니터링할 수 있습니다AWS CLI.

다음 `describe-task-execution`명령을 복사합니다. 이 예시 명령을 사용하려면 *`user input placeholders`*를 실제 정보로 대체하십시오.

```
aws datasync describe-task-execution \
  --task-execution-arn 'arn:aws:datasync:region:account-id:task/task-id/execution/task-execution-id'
```

해당 명령은 다음과 비슷한 작업 실행에 관한 정보를 반환합니다.

```
{
    "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"
    }
}
```

- 작업 실행이 성공하면 상태 값은 성공으로 변경됩니다. 응답 요소의 의미에 대한 자세한 내용은 DescribeTaskExecution을 참조하세요.
- 작업 실행이 실패할 경우, 문제를 해결하는 데 도움이 되는 오류 코드를 그 결과로 전송합니다. 오류 코드에 대한 자세한 내용은 TaskExecutionResultDetail을(를) 참조하십시오.

watch 유틸리티를 사용하여 전송 모니터링

명령줄에서 작업의 진행 상황을 실시간으로 모니터링하려는 경우 표준 Unix watch유틸리티를 사용하면 됩니다. 작업 실행 기간 값은 밀리초 단위로 측정됩니다.

watch유틸리티가 DataSync 별칭을 인식하지 못합니다. 다음 예제는 CLI를 간접적으로 호출하는 방법을 보여줍니다. 이 예시 명령을 사용하려면 *user input placeholders*를 실제 정보로 대체하십시오.

```
# pass '-n 1' to update every second and '-d' to highlight differences
        $ watch -n 1 -d \ "aws datasync describe-task-execution --task-execution-arn
 'arn:aws:datasync:region:account-id:task/task-id/execution/task execution-id'"
```

AWS DataSync 리소스 관리

에이전트, 위치 및 작업과 같은 AWS DataSync 리소스를 관리하는 방법을 알아봅니다.

DataSync 에이전트 관리

DataSync 에이전트를 활성화하면가 에이전트를 자동으로 AWS 관리합니다(소프트웨어 업데이트 포함). 자세히 알아보기

DataSync 에이전트의 연결 및 시스템 리소스 테스트

는 DataSync 에이전트를 배포하고 활성화한 후 AWS 관리하지만 에이전트의 설정을 변경하거나 문제를 해결해야 하는 경우가 있을 수 있습니다. 자세히 알아보기

DataSync 에이전트 교체

DataSync 에이전트를 교체하려면 새 에이전트를 만들고 이전 에이전트를 사용하는 모든 위치를 업데이트해야 합니다. 자세히 알아보기

DataSync 리소스 정리

테스트에 DataSync를 사용했거나 리소스가 더 이상 필요하지 않은 경우, 해당 리소스에 대한 요금이 부과되지 않도록 해당 리소스를 삭제합니다. 자세히 알아보기

DataSync 에이전트의 인프라 재사용

DataSync에서 에이전트 리소스를 삭제한 후에도 에이전트의 가상 머신 또는 Amazon EC2 인스턴스를 사용하여 새 에이전트를 활성화할 수 있습니다. 자세히 알아보기

AWS DataSync 에이전트 관리

AWS DataSync 에이전트를 활성화하면가 가상 머신(VM) 어플라이언스를 관리합니다. AWS

에이전트 소프트웨어 업데이트

AWS 는 기본 운영 체제 및 관련 DataSync 소프트웨어 패키지를 포함하여 에이전트의 소프트웨어를 자동으로 업데이트합니다.

DataSync는 에이전트가 유휴 상태일 때만 에이전트를 업데이트합니다. 예를 들어 전송이 완료될 때까지 에이전트는 업데이트되지 않습니다.

업데이트 후 에이전트가 잠시 오프라인 상태가 될 수 있습니다. 예를 들어, 에이전트를 활성화하고 에이전트를 AWS 업데이트한 직후에 이런 일이 발생할 수 있습니다.

Important

- DataSync는 에이전트를 자동으로 정기 패치하여 보안 및 안정성을 유지합니다. DataSync Basic 모드 에이전트는 Amazon Linux 2를 기본 운영 체제로 사용합니다. DataSync Enhanced 모드 에이전트는 Amazon Linux 2023을 기본 운영 체제로 사용합니다. Amazon Linux 보안 센터에서 탐지된 일반적인 취약성 및 노출(CVE) 문제의 현재 상태를 확인할 수 있습니다. CVE 패치는 Amazon Linux 보안 센터에 표시된 대로, 릴리스 날짜로부터 30일 이내에 자동 적용됩니다. 패치 적용은 에이전트가 온라인 상태이고 작업을 활발히 실행하지 않을 때 진행됩니다.
- DataSync는 cloud-init 지침을 사용하여 Amazon EC2 에이전트를 수동으로 업데이트하는 것을 지원하지 않습니다. 이 방법으로 에이전트를 업데이트하면 에이전트를 활성화하거나 사용할 수 없는 DataSync와의 상호 운용성 문제가 발생할 수 있습니다.

에이전트 상태

다음 표에서는 DataSync 에이전트의 상태를 설명합니다.

에이전트 상태	의미
온라인	에이전트가 적절히 구성되어 사용할 준비가 되었습니다. 에이전트의 정상 실행 상태입니다.
오프라인	에이전트가 5분 이상 DataSync 서비스와 연락이 끊겼습니다. 몇 가지 원인이 있을 수 있습니다. 자세한 내용은 에이전트가 오프라인 상태인 경우, 어떻게 해야 하나요? 섹션을 참조하세요.

에이전트 문제 해결

가 DataSync 에이전트를 자동으로 AWS 관리하지만 해당 에이전트로 다시 직접 작업해야 하는 경우가 있습니다. 예를 들어 에이전트가 오프라인 상태가 되거나 온프레미스 스토리지 시스템과 연결이 끊긴 경우 에이전트의 로컬 콘솔에서 이러한 문제를 해결해 볼 수 있습니다.

자세한 내용은 DataSync 에이전트 문제 해결을 참조하세요.

에이전트에 대한 유지 관리 수행

는 AWS DataSync 에이전트를 배포하고 활성화한 후 AWS 관리하지만 에이전트의 설정을 변경하거나 문제를 해결해야 하는 경우가 있을 수 있습니다. 로컬 콘솔을 통해 에이전트와 협력해야 하는 이유의 몇 가지 예는 다음과 같습니다.

- 에이전트에 IP 주소를 수동으로 할당합니다.
- 에이전트의 시스템 리소스를 점검합니다.

> **Important**
>
> 표준 DataSync 기능은 에이전트의 로컬 콘솔을 사용할 필요가 없습니다.

에이전트의 로컬 콘솔 액세스

로컬 콘솔에 액세스하는 방법은 사용 중인 에이전트 유형에 따라 다릅니다.

로컬 콘솔(VMware ESXi, Linux KVM, Nutanix AHV 또는 Microsoft Hyper-V)에 액세스

보안상의 이유로 DataSync 에이전트 VM(가상 머신)의 로컬 콘솔에 원격으로 연결할 수 없습니다. 하이퍼바이저 관리 인터페이스에서 로컬 콘솔에 액세스해야 합니다.

- 로컬 콘솔에 처음 로그인하는 경우, 임시 자격 증명을 사용하여 로그인합니다. 초기 사용자 이름은 **`admin`**이고, 임시 암호는 **`password`**입니다. 처음 로그인할 때 암호를 변경해야 합니다.

  > **Note**
  >
  > 향상된 모드 에이전트에는 다음과 같은 암호 요구 사항이 있습니다.
  >
  > - 최소 15자를 포함해야 합니다.

- 하나 이상의 대문자를 포함해야 합니다.
- 소문자를 하나 이상 포함해야 합니다.
- 하나 이상의 숫자 문자를 포함해야 합니다.
- 하나 이상의 특수 문자를 포함해야 합니다.
- 암호 업데이트 시 문자의 50% 이상이 변경되어야 합니다.
- 암호는 사전 단어일 수 없습니다.

> **Note**
>
> 초기 암호 설정 후 언제든지 암호를 변경할 수 있습니다. 콘솔 기본 메뉴에서 명령 프롬프트 옆에 번호를 입력한 다음 `passwd` 명령을 실행하여 암호를 변경합니다.

로컬 콘솔 액세스(Amazon EC2)

Amazon EC2 에이전트의 로컬 콘솔에 연결하려면 SSH를 사용해야 합니다.

시작하기 전에: EC2 인스턴스의 보안 그룹이 SSH(TCP 포트 22)를 통한 액세스를 허용하는지 확인합니다.

1. 터미널을 열고 다음 `ssh`명령을 복사합니다.

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

   - */path/key-pair-name*의 경우 인스턴스에 연결하는 데 필요한 프라이빗 키의 경로와 파일 이름(`.pem`)을 지정합니다.
   - *instance-user-name*의 경우 `admin`를 지정합니다.
   - *instance-public-ip-address*의 경우, 인스턴스의 퍼블릭 IP 주소를 지정합니다.
2. `ssh` 명령을 실행하여 인스턴스에 연결합니다.

연결되면 에이전트의 로컬 콘솔 기본 메뉴가 표시됩니다.

에이전트의 DHCP, DNS, IP 설정 구성

에이전트의 기본 네트워크 구성은 DHCP(Dynamic Host Configuration Protocol)입니다. DHCP를 통해 에이전트에 IP 주소가 자동으로 지정됩니다. 다음 설명과 같이 에이전트의 IP를 고정 IP 주소로 수동 지정해야 하는 경우가 있을 수 있습니다.

1. 에이전트의 로컬 콘솔에 로그인합니다.
2. 네트워크 구성을 시작하려면 AWS DataSync 활성화 - 구성 기본 메뉴에서 **1**을 입력합니다.
3. Network Configuration(네트워크 구성) 메뉴에서 다음 옵션 중 하나를 선택하십시오.

목적	조치

네트워크 어댑터에 대한 정보 얻기	**1**을 입력합니다.
	
	어댑터 이름 목록이 나타나고 어댑터 이름을 입력하라는 메시지가 표시됩니다(예: **eth0**). 지정한 어댑터가 사용 중인 경우, 어댑터에 대한 네트워크 정보가 다음 예시와 같이 표시됩니다.
	
	`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`

목적	조치
	고정 IP 주소를 구성할 경우(옵션 3), 에이전트의 기본 경로 어댑터를 설정할 때(옵션 5)와 동일한 어댑터 이름을 사용합니다.
DHCP 구성	**2**을 입력합니다. 사용할 IP 버전을 선택한 다음 DHCP를 사용하도록 네트워크 인터페이스를 구성합니다.
에이전트에 고정 IP 주소 구성	**3**을 입력합니다. 사용할 IP 프로토콜을 IPv4, IPv6 또는 둘 다 선택하라는 메시지가 표시됩니다. 그런 다음 네트워크 어댑터 이름을 입력하여 고정 IP 주소를 구성하라는 메시지가 표시됩니다. **Important** 에이전트가 이미 활성화된 경우, 설정이 적용되도록 DataSync 콘솔에서 에이전트를 종료한 후 다시 시작해야 합니다.

목적	조치
에이전트의 모든 네트워크 구성을 DHCP로 재설정	**4**을 입력합니다. DHCP로 재설정할 IP 버전을 선택합니다. 선택한 IP 버전의 모든 네트워크 인터페이스는 DHCP를 사용하도록 설정됩니다. **Important** 에이전트가 이미 활성화된 경우, 설정이 적용되도록 DataSync 콘솔에서 에이전트를 종료한 후 다시 시작해야 합니다.
에이전트의 기본 경로 어댑터 설정	**5**을 입력합니다. 에이전트에 사용할 수 있는 어댑터가 표시되고 어댑터 중 하나를 선택하라는 메시지가 표시됩니다(예: **eth0**).
에이전트의 도메인 이름 시스템(DNS) 구성 편집	**6**을 입력합니다. 주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다. 새 IP 주소를 제공하라는 메시지가 나타납니다.

목적	조치
에이전트 DSN 구성 보기	**7**을 입력합니다. 주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다. **Note** 일부 VMware 하이퍼바이저 버전은 이 메뉴에서 어댑터 구성을 편집할 수 있습니다.
라우팅 테이블 조회	**8**을 입력합니다. IP 버전(IPv4, IPv6 또는 둘 다)을 선택하여 에이전트의 기본 라우팅 테이블을 확인합니다.
데이터 전송을 위해 에이전트의 IP 버전 보기	**9**을 입력합니다. 데이터 전송을 위한 에이전트의 IP 버전 설정은 `IPv4`, `IPv6`, `IPv4 (auto)`, `IPv6 (auto)`로 표시됩니다.
데이터 전송을 위해 에이전트의 IP 프로토콜 편집	**10**을 입력합니다. 데이터 전송에 사용할 수 있는 IP 버전 설정이 표시됩니다. `IPv4`, `IPv6`, `IPv4 (auto)`, `IPv6 (auto)` 중 하나를 선택할 수 있습니다. 데이터 전송을 위한 에이전트의 IP 버전 설정에 대한 자세한 내용은 the section called “IPv6 지원”을 참조하세요.

에이전트의 시스템 리소스 점검

에이전트 콘솔에 로그인하면 가상 CPU 코어, 루트 볼륨 크기 및 RAM이 자동으로 확인됩니다. 오류나 경고가 있는 경우 콘솔 메뉴 디스플레이에 해당 오류나 경고에 대한 세부 정보를 제공하는 배너와 함께 플래그가 표시됩니다.

콘솔 시작 시 오류나 경고가 없는 경우 메뉴에 흰색 텍스트가 표시됩니다. 시스템 리소스 점검 조회 옵션에 `(0 Errors)`이 표시됩니다.

오류나 경고가 있는 경우 콘솔 메뉴의 메뉴 상단에 있는 배너에 오류와 경고 수가 각각 빨간색과 노란색으로 표시됩니다. 예를 들어 `(1 ERROR, 1 WARNING)`입니다.

에이전트의 시스템 리소스를 점검하려면

1. 에이전트의 로컬 콘솔에 로그인합니다.
2. 시스템 리소스 점검 결과를 확인하려면 AWS DataSync 활성화 - 구성 기본 메뉴에서 **4**을 입력합니다.

   다음 표의 설명처럼 콘솔에서 각 리소스에 [확인], [경고] 또는 [실패] 메시지가 표시됩니다.

   Amazon EC2 인스턴스에 대해 시스템 리소스 점검을 통해 인스턴스 유형이 DataSync와 함께 사용하도록 권장되는 인스턴스 중 하나인지 확인합니다. 인스턴스 유형이 해당 목록과 일치하면 다음과 같이 단일 결과가 녹색 텍스트로 표시됩니다.

   ```
   [ OK ] Instance Type Check
   ```

   Amazon EC2 인스턴스가 권장 목록에 없는 경우 시스템 리소스 점검을 통해 다음 리소스를 확인합니다.

   - CPU 코어 점검: 4개 이상의 코어가 필요합니다.
   - 디스크 크기 점검: 최소 80GB의 사용 가능한 디스크 공간이 필요합니다.
   - RAM 점검:
     - 최대 2천만 개의 파일, 객체 또는 디렉토리를 처리하는 작업을 실행할 수 있도록 32GB RAM이 인스턴스에 할당.
     - 2천만 개 이상의 파일, 객체 또는 디렉토리를 처리하는 작업을 실행할 수 있도록 64GB RAM이 인스턴스에 할당.
   - CPU 플래그 점검: 에이전트 VM CPU에는 SSSE3 또는 SSE4 명령 세트 플래그가 있어야 합니다.

Amazon EC2 인스턴스가 DataSync의 권장 인스턴스 목록에 없지만 리소스가 충분한 경우, 시스템 리소스 점검 결과는 4개의 결과를 모두 녹색 텍스트로 표시합니다.

Hyper-V, Linux 커널 기반 가상 머신(KVM) 및 VMware VM에 배포된 에이전트에 대해서도 동일한 리소스가 검증됩니다.

또한 VMware 에이전트의 지원되는 버전을 확인합니다. 지원되지 않는 버전에서는 빨간색 배너 오류가 발생합니다. 지원되는 버전에는 VMware 버전 6.5 및 6.7이 포함됩니다.

에이전트 시스템 시간 서버 구성 보기 및 관리

에이전트의 시스템 시간 서버 구성을 보고 관리할 수 있습니다.

1. 에이전트의 로컬 콘솔에 로그인합니다.
2. AWS DataSync 활성화 - 구성 기본 메뉴에서 시스템 시간 관리에 대한 옵션(예: VMware 에이전트의 경우 **5**)을 입력합니다.
3. 시스템 시간 관리 메뉴에서 다음 중 하나를 선택합니다.

목적	조치
시스템 시간 및 서비스 상태 보기	**1**을 입력합니다. 현재 시스템 시간을 UTC, 시간 서비스 상태, 활성 시간 서버, 동기화 상태로 확인합니다.
시스템 시간 동기화	**2**을 입력합니다. 시간 서버를 즉시 동기화하라는 프롬프트가 표시됩니다. 경우에 따라 에이전트의 시간이 변동될 수 있습니다. 예를 들어 네트워크 중단이 길어지고 하이퍼바이저 호스트와 에이전트가 시간 업데이트를 받지 못하므로 에이전트의 시간이 실제 시간과 다를 수 있습니다. 이렇게 시간 오차가 있는 경우, 작업(스냅샷 발생 등)이 실행되도록 지정

목적	조치
	한 시간과 작업이 실제 이루어지는 시간 사이에 불일치가 발생합니다.
시스템 시간 서비스 다시 시작	**3**을 입력합니다. 시간 동기화 서비스를 다시 시작하라는 프롬프트가 표시됩니다.
시간 서버 구성 관리	**4**을 입력합니다. 시간 서버 설정을 확인하고 관리합니다. 시간 서버 및 서버 풀을 추가 또는 제거하고 정확한 동기화를 위해 기본 서버를 설정합니다.

에이전트에 대한 유지 관리 관련 명령 실행

DataSync 에이전트의 로컬 콘솔에서 일부 유지 관리 작업을 수행하고 에이전트와 함께 문제를 진단할 수 있습니다.

에이전트의 로컬 콘솔에서 구성 또는 진단 명령을 실행하려면

1. 에이전트의 로컬 콘솔에 로그인합니다.
2. AWS DataSync 활성화 - 구성 기본 메뉴에서 명령 프롬프트에 **5**(또는 VMware VM의 경우 **6**)를 입력합니다.
3. 다음 명령을 사용하여 에이전트와 함께 다음 작업을 수행합니다.

명령	설명
dig	호스트 DNS 정보를 조회합니다.
diskclean	디스크 정리를 수행합니다.
exit	콘솔 구성 메뉴로 돌아갑니다.
h	사용 가능한 명령 목록을 표시합니다.

명령	설명
ifconfig	네트워크 인터페이스를 표시하거나 구성합니다.
ip	라우팅, 디바이스, 터널을 표시하거나 구성합니다.
iptables	IPv4 패킷 필터링 및 NAT를 설정하고 유지 관리합니다.
ip6tables	IPv6 패킷 필터링 및 NAT를 설정하고 유지 관리합니다.
ncport	특정 네트워크 TCP 포트에 대한 연결을 테스트합니다.
nping	네트워크 문제를 해결하기 위한 정보를 얻습니다.
passwd	사용자 암호를 변경합니다.
save-iptables	IPv4 테이블 방화벽 규칙을 영구적으로 저장합니다.
save-ip6tables	IPv6 테이블 방화벽 규칙을 영구적으로 저장합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.
sslcheck	SSL 인증서가 유효한지 확인합니다.
tcptraceroute	대상으로 향하는 TCP 트래픽의 `traceroute` 출력을 수집합니다.

4. 화면에 표시되는 지시 사항을 따릅니다.

AWS DataSync 에이전트 교체

AWS DataSync 에이전트를 교체하려면 새 에이전트를 만들고 이전 에이전트를 사용하는 모든 이동 위치를 업데이트해야 합니다.

새 에이전트 만들기

새 DataSync 에이전트를 만들려면 이전 에이전트를 만들 때와 동일한 프로세스를 따르세요.

1. 스토리지 환경에 에이전트를 배포하세요.
2. AWS와 통신하기 위해 에이전트가 사용하는 서비스 엔드포인트를 선택하십시오.
3. 에이전트가 귀하의 스토리지 및 AWS과 통신할 수 있도록 귀하의 네트워크를 구성하세요.
4. 에이전트를 활성화하십시오.
5. 활성화되면 에이전트의 Amazon 리소스 이름(ARN)을 기록해 둡니다.

   새 에이전트를 사용하기 위해 DataSync 위치를 업데이트할 때 이 ARN이 필요합니다.

새 에이전트를 통한 위치 업데이트

새 에이전트를 만든 후에는 기존 DataSync 위치를 업데이트하여 이 에이전트를 사용할 수 있습니다. 대부분의 경우, 위치를 업데이트하려면 액세스 자격 증명도 다시 입력해야 합니다. 이는 DataSync가 에이전트만 사용할 수 있는 방식으로 위치 자격 증명을 저장하기 때문입니다.

DataSync 콘솔 사용

다음 지침은 DataSync 콘솔을 사용하여 새 에이전트로 위치를 업데이트하는 방법을 설명합니다.

NFS

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 위치를 선택합니다.
3. 업데이트할 위치를 선택한 후 편집을 선택합니다.
4. 에이전트의 경우, 새 에이전트를 선택하세요.

   한 위치의 여러 에이전트를 교체하는 경우, 하나 이상의 에이전트를 선택할 수 있습니다.
5. 변경 사항 저장을 선택합니다.

SMB

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 위치를 선택합니다.
3. 업데이트할 위치를 선택한 후 편집을 선택합니다.

4. 에이전트의 경우, 새 에이전트를 선택하세요.

   한 위치의 여러 에이전트를 교체하는 경우, 하나 이상의 에이전트를 선택할 수 있습니다.
5. 암호에는 SMB 파일 서버를 탑재할 수 있고 전송과 관련된 파일 및 폴더에 액세스할 수 있는 권한을 가진 사용자의 암호를 입력합니다.
6. 변경 사항 저장을 선택합니다.

HDFS

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 위치를 선택합니다.
3. 업데이트할 위치를 선택한 후 편집을 선택합니다.
4. 에이전트의 경우, 새 에이전트를 선택하세요.

   한 위치의 여러 에이전트를 교체하는 경우, 하나 이상의 에이전트를 선택할 수 있습니다.
5. Kerberos 인증을 사용하는 경우, Keytab 파일과 Kerberos 구성 파일을 업로드하세요.
6. 변경 사항 저장을 선택합니다.

Object storage

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 위치를 선택합니다.
3. 업데이트할 위치를 선택한 후 편집을 선택합니다.
4. 에이전트의 경우, 새 에이전트를 선택하세요.

   한 위치에 대해 복수의 에이전트를 교체하는 경우, 둘 이상의 에이전트를 선택할 수 있습니다.
5. 해당 위치에서 자격 증명이 필요한 경우 DataSync가 객체 스토리지 버킷에 액세스하도록 허용하는 보안 키를 입력합니다.
6. 변경 사항 저장을 선택합니다.

Azure Storage

Microsoft Azure Blob Storage 위치를 업데이트하려면 다음을 수행하세요.

1. https://console.aws.amazon.com/datasync/에서 AWS DataSync콘솔을 엽니다.

2. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 위치를 선택합니다.
3. 업데이트할 위치를 선택한 후 편집을 선택합니다.
4. 에이전트의 경우, 새 에이전트를 선택하세요.

   한 위치에 대해 복수의 에이전트를 교체하는 경우, 둘 이상의 에이전트를 선택할 수 있습니다.
5. SAS 토큰의 경우, DataSync가 Blob 스토리지에 액세스할 수 있도록 허용하는 공유 액세스 서명(SAS) 토큰을 입력합니다.
6. 변경 사항 저장을 선택합니다.

AWS CLI 사용

다음 지침은 AWS CLI를 사용하여 새 에이전트로 위치를 업데이트하는 방법을 설명합니다. (이 작업은 DataSync API를 사용하여 수행할 수도 있습니다.)

NFS

1. 다음 update-location-nfs 명령을 복사하세요.

```
aws datasync update-location-nfs \
  --location-arn datasync-nfs-location-arn \
  --on-prem-config AgentArns=new-datasync-agent-arn
```

2. `--location-arn` 파라미터에는 업데이트하려는 NFS 위치의 ARN을 지정합니다.
3. `--on-prem-config` 파라미터 `AgentArns`옵션에는 새 에이전트의 ARN을 지정합니다.

   한 위치에 대해 복수의 에이전트를 교체하는 경우, 둘 이상의 ARN을 지정할 수 있습니다.
4. `update-location-nfs` 명령을 실행하여 위치를 업데이트합니다.

SMB

1. 다음 update-location-smb 명령을 복사하세요:

```
aws datasync update-location-smb \
  --location-arn datasync-smb-location-arn \
  --agent-arns new-datasync-agent-arn \
  --password smb-file-server-password
```

2. `--location-arn` 파라미터에는 업데이트하려는 SMB 위치의 ARN을 지정합니다.

3. `--agent-arns` 파라미터에는 새 에이전트의 ARN을 지정합니다.

   한 위치에 대해 복수의 에이전트를 교체하는 경우, 둘 이상의 ARN을 지정할 수 있습니다.

4. `--password` 파라미터의 경우, SMB 파일 서버를 탑재할 수 있고 전송과 관련된 파일 및 폴더에 액세스할 수 있는 권한을 가진 사용자의 비밀번호를 지정하세요.

5. `update-location-smb` 명령을 실행하여 위치를 업데이트합니다.

HDFS

1. 다음 update-location-hdfs 명령을 복사합니다.

```
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. `--location-arn` 파라미터에는 업데이트하려는 HDFS 위치의 ARN을 지정합니다.

3. `--agent-arns` 파라미터에는 새 에이전트의 ARN을 지정합니다.

   한 위치의 여러 에이전트를 교체하는 경우, 하나 이상의 ARN을 지정할 수 있습니다.

4. Kerberos 인증을 사용하는 경우, `--kerberos-keytab`및 `--kerberos-krb5-conf`파라미터를 포함하세요.

   - `--kerberos-keytab` 파라미터의 경우, 정의된 Kerberos 보안 주체와 암호화된 키 사이의 매핑이 포함된 Kerberos 키 테이블(keytab)을 지정합니다.

     파일 주소를 제공하여 keytab 파일을 지정할 수 있습니다.

   - `--kerberos-krb5-conf` 파라미터에는 Kerberos 영역에 대한 구성이 포함된 파일을 지정하세요.

     `krb5.conf` 파일은 파일 주소를 제공함으로써 지정할 수 있습니다.

   단순 인증을 사용하는 경우, 명령에 이러한 Kerberos 관련 파라미터를 포함하지 않아도 됩니다.

5. `update-location-hdfs` 명령을 실행하여 위치를 업데이트합니다.

Object storage

1. 다음 update-location-object-storage 명령을 복사합니다.

```
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. `--location-arn` 파라미터에는 업데이트하려는 객체 스토리지 위치의 ARN을 지정합니다.
3. `--agent-arns` 파라미터에는 새 에이전트의 ARN을 지정합니다.

   한 위치의 여러 에이전트를 교체하는 경우, 하나 이상의 ARN을 지정할 수 있습니다.
4. 객체 스토리지 위치에 액세스 자격 증명이 필요한지 여부에 따라 다음을 수행합니다.

   - 위치에 자격 증명이 필요한 경우 - `--secret-key` 파라미터에는 DataSync가 객체 스토리지 버킷에 액세스할 수 있는 보안 키를 지정합니다.
   - 위치에 자격 증명이 필요한 경우 - `--access-key` 및 `--secret-key` 파라미터에 빈 문자열을 지정합니다. 다음은 명령의 예입니다.

```
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. `update-location-object-storage` 명령을 실행하여 위치를 업데이트합니다.

Azure Storage

1. 다음 update-location-azure-blob 명령을 복사하세요.

```
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. `--location-arn` 파라미터에는 업데이트하려는 Azure Blob Storage위치의 ARN을 지정합니다.
3. `--agent-arns` 파라미터에는 새 에이전트의 ARN을 지정합니다.

   한 위치의 여러 에이전트를 교체하는 경우, 하나 이상의 ARN을 지정할 수 있습니다.
4. `--sas-configuration` 파라미터 `Token`옵션의 경우, DataSync가 Blob 스토리지에 액세스할 수 있도록 허용하는 SAS 토큰을 지정합니다.
5. `update-location-azure-blob` 명령을 실행하여 위치를 업데이트합니다.

다음 단계

1. 이전 에이전트를 삭제하세요. 이 에이전트를 사용하여 DataSync 작업을 실행 중인 경우, 해당 작업이 완료될 때까지 기다렸다가 삭제하세요.
2. 여러 위치의 에이전트를 교체해야 하는 경우, 이전 단계를 반복하세요.
3. 작업을 마치면 작업 실행을 재개할 수 있습니다.

> **Note**
>
> 예약된 작업의 에이전트 교체 - 예약된 작업의 에이전트를 교체하는 경우 새 에이전트가 이전 에이전트와 다른 유형의 서비스 엔드포인트를 사용하는 경우 해당 작업을 수동으로 시작해야 합니다. 예약된 다음 실행 전에 작업을 수동으로 실행하지 않으면 작업이 실패합니다.
> 예를 들어 이전 에이전트가 퍼블릭 서비스 엔드포인트를 사용했지만 새 에이전트가 VPC 엔드포인트를 사용하는 경우 콘솔 또는 `StartTaskExecution` 작업을 사용하여 해당 작업을 수동으로 시작합니다. 그런 다음 작업이 일정에 따라 재개됩니다.

AWS DataSync 리소스 필터링

의 및 `ListTasks` API 작업을 사용하여 AWS DataSync 위치 `ListLocations` 및 작업을 필터링할 수 있습니다 AWS CLI. 예를 들어 가장 최근 작업 목록을 검색할 수 있습니다.

필터링을 위한 파라미터

API 필터를 사용하여 `ListTasks`및 `ListLocations`에서 반환되는 리소스 목록의 범위를 좁힐 수 있습니다. 예를 들어, 모든 Amazon S3 위치를 검색하려면 `ListLocations`을 필터 이름 `LocationType`*`S3`*과 `Operator`*`Equals`* 함께 사용할 수 있습니다.

API 결과를 필터링하려면 필터 이름, 연산자 및 값을 지정해야 합니다.

- `Name` – 사용 중인 필터의 이름입니다. 각 API 직접 호출은 사용할 수 있는 필터 목록을 지원합니다(예: `ListLocations`에 대한 `LocationType`).
- `Values` – 필터링 기준으로 사용할 값입니다. 예컨대, Amazon S3 위치만 표시할 수 있습니다.
- `Operator` – 필터 값을 비교하는 데 사용되는 연산자입니다(예: `Equals`또는`Contains`).

다음 표에는 이용 가능한 연산자가 나열되어 있습니다.

연산자	키 유형
`Equals`	문자열, 숫자
`NotEquals`	문자열, 숫자
`LessThan`	숫자
`LessThanOrEqual`	숫자
`GreaterThan`	숫자
`GreaterThanOrEqual`	숫자
`In`	문자열
`Contains`	문자열
`NotContains`	문자열
`BeginsWith`	문자열

위치별 필터링

ListLocations(은)는 다음 필터 이름을 지원합니다.

- LocationType – 위치 유형에 따른 필터:
  - SMB
  - NFS
  - HDFS
  - OBJECT_STORAGE
  - S3
  - OUTPOST_S3
  - FSX_WINDOWS
  - FSX_LUSTRE
  - FSX_OPENZFS_NFS
  - FSX_ONTAP_NFS
  - FSX_ONTAP_SMB
- LocationUri – DescribeLocation*API 직접 호출에서 반환된 대로 위치에 할당된 URI(Uniform Resource Identifier)에 대한 필터(예: Amazon S3 위치에 대한 s3://*bucket-name*/*your-prefix*).
- CreationTime – 위치가 생성된 시간에 대한 필터. 입력 형식은 국제 표준시(UTC)의 yyyy-MM-dd:mm:ss입니다.

다음 AWS CLI 예제에서는 문자열로 시작하고 2019-12-15 17:15:20 UTC 이후에 생성된 위치 URI가 "s3://amzn-s3-demo-bucket" 있는 Amazon S3 유형의 모든 위치를 나열합니다.

```
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}]
```

다음과 비슷한 출력이 반환됩니다.

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

작업 기준으로 필터링

ListTasks(은)는 다음 필터 이름을 지원합니다.

- LocationId – Amazon 리소스 이름(ARN) 값의 소스 및 대상 위치 둘 다에 대한 필터.
- CreationTime – 작업이 생성된 시간에 대한 필터. 입력 형식은 UTC의 yyyy-MM-dd:mm:ss입니다.

다음 AWS CLI 예제에서는에서 필터링할 때의 구문을 보여줍니다LocationId.

```
aws datasync list-tasks \
    --filters Name=LocationId,Values=arn:aws:datasync:us-east-1:your-account-
id:location/your-location-id,Operator=Contains
```

이 명령의 출력은 다음과 비슷합니다.

```
{
    "Tasks": [
        {
            "TaskArn": "arn:aws:datasync:us-east-1:your-account-id:task/your-task-id",
            "Status": "AVAILABLE",
            "Name": "amzn-s3-demo-bucket"
        }
    ]
}
```

AWS DataSync 리소스 정리

테스트 AWS DataSync 에를 사용했거나 생성한 AWS 리소스가 필요하지 않은 경우 사용하지 않을 리소스에 대한 요금이 부과되지 않도록 삭제합니다.

> **Note**
>
> 비활성화한 옵트인 리전에 DataSync 리소스가 있는 경우 해당 리소스는 자동으로 삭제되지 않습니다. 해당 리전을 다시 활성화해도 리소스는 여전히 남아 있습니다.

DataSync 에이전트 삭제

에서 에이전트를 삭제하면 AWS DataSync에이전트 리소스가 더 이상 AWS 계정 와 연결되지 않으며 실행 취소할 수 없습니다.

DataSync에서 에이전트를 삭제해도 스토리지 환경에서 가상 머신(VM) 또는 Amazon EC2 인스턴스가 제거되지는 않는다는 점에 유의하세요. VM 또는 인스턴스를 삭제하거나 재사용하여 새 에이전트를 활성화할 수 있습니다.

사전 조건

에이전트에 종속된 DataSync 리소스를 업데이트하거나 제거할 때까지 에이전트를 삭제하지 마세요. 에이전트를 교체하는 경우 전송 위치를 새 에이전트로 업데이트하세요. 에이전트를 교체하지 않을 경우 먼저 해당 에이전트를 이용한 이동 작업과 위치를 삭제하세요.

에이전트 삭제

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 에이전트를 선택합니다.
3. 삭제하려는 에이전트를 선택합니다.
4. 삭제를 선택하고 텍스트 상자가 나타나면 **`delete`**를 입력한 후, 삭제를 선택합니다.
5. 다른 DataSync 활동에 에이전트 인프라를 재사용할 계획이 없는 경우 에이전트의 VM 또는 Amazon EC2 인스턴스를 삭제하고 스토리지 환경에서 제거합니다.

DataSync 에이전트의 인프라 재사용

DataSync에서 에이전트 리소스를 삭제한 후에도 에이전트의 기본 VM 또는 Amazon EC2 인스턴스를 사용하여 새 에이전트를 활성화할 수 있습니다.

에이전트의 인프라를 재사용하려면

1. 에이전트의 연결을 테스트합니다 AWS. 네트워크 테스트가 통과하면 다음 단계로 이동합니다.

   다음 단계로 이동하려면 네트워크 테스트를 통과해야 합니다.
2. DataSync에서 에이전트 리소스를 삭제하되 에이전트의 VM 또는 Amazon EC2 인스턴스는 삭제하지 마세요.
3. 1단계를 반복하여 에이전트의에 대한 연결을 AWS 다시 테스트합니다. 네트워크 테스트가 통과하면 다음 단계로 이동합니다.
4. DataSync에서 에이전트 리소스를 삭제한 후 약 3분 후에 에이전트 VM 또는 Amazon EC2 인스턴스에서 포트 80이 열려 있는지 확인합니다. 만일 그렇다면, 다음 단계로 이동합니다.
5. 기존 VM 또는 Amazon EC2 인스턴스로 새 에이전트를 활성화합니다.

   다른 및 AWS 리전 AWS 계정다른 유형의 서비스 엔드포인트에서 새 에이전트를 활성화할 수 있습니다. 다른 유형의 서비스 엔드포인트를 사용하는 경우 네트워크 구성을 조정해야 합니다.

DataSync 위치 삭제

더 이상 필요하지 않은 AWS DataSync 위치를 제거하는 것이 가장 좋습니다.

DataSync 콘솔을 사용하여 위치를 제거하려면

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 위치를 선택합니다.
3. 제거할 위치를 선택합니다.
4. 삭제를 선택합니다. **`delete`**을(를) 입력해서 삭제를 확인한 후 삭제를 선택합니다.

DataSync 작업 삭제

작업이 더 이상 필요하지 않은 경우 해당 AWS DataSync 작업과 관련 AWS 리소스를 삭제할 수 있습니다.

사전 조건

태스크를 실행하면 DataSync는 전송을 위한 데이터 트래픽을 관리하기 위한 네트워크 인터페이스를 생성합니다. 태스크를 삭제하면 다음과 같은 권한이 있는 한 관련 네트워크 인터페이스도 삭제됩니다.

- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`

이러한 권한은 AWS 관리형 정책에서 사용할 수 있습니다`AWSDataSyncFullAccess`. 자세한 내용은 AWS 에 대한 관리형 정책 AWS DataSync 단원을 참조하십시오.

태스크 삭제

태스크를 삭제하면 복원할 수 없습니다.

DataSync 콘솔 사용

1. https://console.aws.amazon.com/datasync/ AWS DataSync 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음, 태스크를 선택합니다.
3. 삭제할 태스크를 선택합니다.
4. 실행을 선택하고 삭제를 선택합니다.
5. 대화 상자에서 삭제를 선택합니다.

사용 AWS CLI

1. 다음 `delete-task`명령을 복사합니다.

```
aws datasync delete-task \
      --task-arn "task-to-delete"
```

2. `--task-arn`파라미터에는 삭제하려는 태스크의 Amazon 리소스 이름(ARN)을 지정합니다(예: `arn:aws:datasync:us-east-2:123456789012:task/task-012345678abcd0123`).
3. `delete-task` 명령을 실행합니다.

의 보안 AWS DataSync

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 클라우드에서 AWS AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사원은 정기적으로 AWS 규제 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS DataSync에 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램 제공 범위 내AWS 서비스를 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 DataSync 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제는 보안 및 규정 준수 목표를 충족하도록 DataSync를 구성하는 방법을 보여줍니다. 또한 DataSync 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- 의 데이터 보호 AWS DataSync
- 의 자격 증명 및 액세스 관리 AWS DataSync
- 의 규정 준수 검증AWS DataSync
- AWS DataSync의 복원성
- AWS DataSync에서 인프라 보안
- Secrets Manager를 사용하여 스토리지 위치 자격 증명 보호

의 데이터 보호 AWS DataSync

AWS DataSync 는 자체 관리형 스토리지 시스템과 AWS 스토리지 서비스 간에는 물론 AWS 스토리지 서비스 간에도 데이터를 안전하게 전송합니다. 전송 시 스토리지 데이터를 암호화하는 방법은 전송과 관련된 위치에 따라 부분적으로 달라집니다.

전송이 완료되면 데이터를 저장하는 시스템 또는 서비스(DataSync 아님) 에서 데이터를 암호화합니다.

주제

- AWS DataSync 전송 중 암호화
- AWS DataSync 저장 시 암호화
- 인터네트워크 트래픽 개인 정보

AWS DataSync 전송 중 암호화

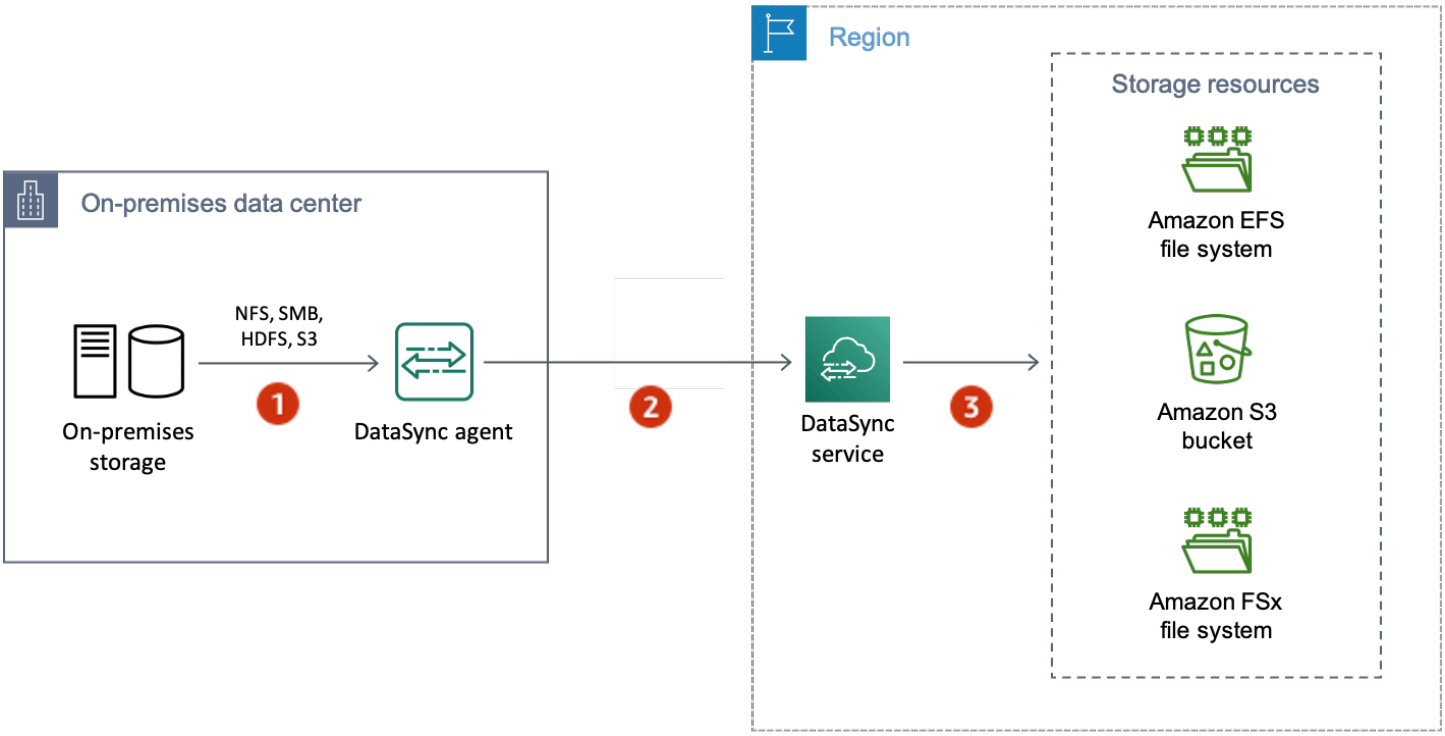
저장 데이터(메타데이터 포함) 는 전송 중에 암호화되지만 전송 과정에서 암호화되는 방식은 원본 및 대상 위치에 따라 다릅니다.

특정 위치에 연결할 때 DataSync는 해당 위치의 데이터 액세스 프로토콜이 제공하는 가장 안전한 옵션을 사용합니다. 예를 들어, 서버 메시지 블록(SMB) 을 사용하여 파일 시스템에 연결할 때 DataSync는 SMB에서 제공하는 보안 기능을 사용합니다.

전송 시 네트워크 연결

DataSync에서 데이터를 복사하려면 세 개의 네트워크 연결이 필요합니다. 하나는 소스 위치에서 데이터를 읽는 연결이고, 다른 하나는 위치 간에 데이터를 전송하는 연결이며, 또 다른 하나는 대상 위치에 데이터를 쓰기 위한 연결입니다.

다음 다이어그램은 DataSync가 온프레미스 스토리지 시스템에서 AWS 스토리지 서비스로 데이터를 전송하는 데 사용하는 네트워크 연결의 예입니다. 연결이 발생하는 위치와 각 연결을 통해 전송하는 데이터를 보호하는 방법을 이해하려면 다음 표를 사용하세요.



레퍼런스	네트워크 연결	설명
1	소스 위치에서 데이터 읽기	DataSync는 데이터에 액세스하는 데 스토리지 시스템의 프로토콜(예: SMB 또는 Amazon S3 API) 을 사용하여 연결합니다. 이 연결에서는 스토리지 시스템의 보안 기능을 사용하여 데이터를 보호합니다(DataSync가 이러한 기능을 지원하지 않는 경우 제외). 예를 들어 DataSync는 현재 NFS 파일 서버를 사용한 Kerberos 인증을 지원하지 않거나, HDFS와 함께 TDE 암호화를 사용할 때 해당 인증을 지원하지 않습니다.
2	위치 간 데이터 전송	이 연결에서 DataSync는 상호 전송 계층 보안(mTLS) 1.3을 사용하여 모든 네트워크 트래픽을 암호화합니다.
3	대상 위치에 데이터 쓰기	소스 위치와 마찬가지로, DataSync는 데이터 액세스를 위해 스토리지 시스

레퍼런스	네트워크 연결	설명
		템 프로토콜을 사용하여 연결합니다. 이번에도 스토리지 시스템의 보안 기능을 사용하여 데이터를 보호합니다 (DataSync가 이러한 기능을 지원하지 않는 경우 제외).

DataSync가 다음 AWS 스토리지 서비스에 연결될 때 전송 중 데이터를 어떻게 암호화 하는지 알아보세요.

- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP
- Amazon S3

TLS 싸이퍼

위치 간에 데이터를 전송할 때 DataSync는 서로 다른 TLS 암호를 사용합니다. TLS 암호는 에이전트가 DataSync와 통신하는 데 사용하는 서비스 엔드포인트의 유형에 따라 달라집니다. (자세한 내용은 AWS DataSync 에이전트의 서비스 엔드포인트 선택 섹션을 참조하세요.)

목차

- 퍼블릭 또는 VPC 엔드포인트
- FIPS 엔드포인트

퍼블릭 또는 VPC 엔드포인트

퍼블릭 및 가상 프라이빗 클라우드(VPC) 서비스 엔드포인트의 경우 DataSync는 다음 TLS 암호 중 하나를 사용합니다.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519)

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519)

FIPS 엔드포인트

Federal Information Processing Standard(FIPS) 서비스 엔드포인트의 경우 DataSync는 다음 TLS 암호를 사용합니다.

- TLS_AES_128_GCM_SHA256(secp256r1)

AWS DataSync 저장 시 암호화

AWS DataSync 는 전송 서비스이므로 일반적으로 저장 스토리지 데이터를 관리하지 않습니다. DataSync가 지원하는 스토리지 서비스 및 시스템은 해당 상태의 데이터를 보호할 책임이 있습니다. 하지만 DataSync가 저장 상태에서 관리하는 일부 서비스 관련 데이터도 있습니다.

무엇을 암호화하나요?

DataSync가 저장 상태로 처리하는 유일한 데이터는 전송을 완료하는 데 필요한 세부 정보와 관련됩니다. DataSync는 Amazon DynamoDB에 완전 저장 상태의 암호화를 적용하여 다음 데이터를 저장합니다.

- 작업 구성(예: 전송 위치에 대한 세부 정보).
- DataSync 에이전트가 위치를 인증할 수 있도록 하는 사용자 자격 증명. 이러한 자격 증명은 에이전트의 공개 키를 사용하여 암호화됩니다. 에이전트는 필요에 따라 개인 키를 사용하여 이러한 키를 해독할 수 있습니다.

자세한 내용을 알아보려면 Amazon DynamoDB 개발자 안내서의 저장 중 DynamoDB 암호화를 참조하세요.

키 관리

DataSync가 작업 실행과 관련된 정보를 DynamoDB에 저장하는 데 사용하는 암호화 키는 관리할 수 없습니다. 이 정보에는 에이전트가 스토리지 위치를 인증하는 데 사용하는 작업 구성 및 자격 증명이 포함됩니다.

암호화되지 않는 것은 무엇인가요?

DataSync가 저장 시 스토리지 데이터를 암호화하는 방식을 제어하지는 않지만 지원하는 최고 수준의 보안으로 위치를 구성하는 것이 좋습니다. 예를 들어 Amazon S3 관리형 암호화 키(SSE-S3) 또는 AWS Key Management Service (AWS KMS) 키(SSE-KMS)를 사용하여 객체를 암호화할 수 있습니다.

AWS 스토리지 서비스가 저장 데이터를 암호화하는 방법에 대해 자세히 알아봅니다.

- Amazon S3
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre
- Amazon FSx for OpenZFS
- Amazon FSx for NetApp ONTAP

인터네트워크 트래픽 개인 정보

소스 및 대상 위치는 각 위치에서 지원하는 최고 수준의 보안으로 구성하는 것이 좋습니다. 위치에 연결할 때 AWS DataSync 는 스토리지 시스템에서 사용하는 가장 안전한 버전의 데이터 액세스 프로토콜을 사용합니다. 또한 서브넷 트래픽을 알려진 프로토콜 및 서비스로 제한하는 것도 고려해 보세요.

DataSync는 전송 계층 보안(TLS) 1.3을 사용하여 AWS 계정 AWS 리전, 및 가용 영역을 포함한 위치 간 연결을 보호합니다.

의 자격 증명 및 액세스 관리 AWS DataSync

AWS 는 보안 자격 증명을 사용하여 사용자를 식별하고 리소스에 대한 AWS 액세스 권한을 부여합니다. AWS Identity and Access Management (IAM)의 기능을 사용하면 보안 자격 증명을 공유하지 않고도 다른 사용자, 서비스 및 애플리케이션이 AWS 리소스를 완전히 또는 제한된 방식으로 사용할 수 있습니다.

기본적으로 IAM 자격 증명(사용자, 그룹 및 역할)에는 AWS 리소스를 생성, 확인 또는 수정할 수 있는 권한이 없습니다. 사용자, 그룹 및 역할이 AWS DataSync 리소스에 액세스하고 DataSync 콘솔 및 API와 상호 작용하도록 허용하려면 필요한 특정 리소스 및 API 작업을 사용할 수 있는 권한을 부여하는 IAM 정책을 사용하는 것이 좋습니다. 그런 다음, 액세스가 필요한 IAM 보안 인증에 정책을 연결합니다. 정책의 기본 요소를 개략적으로 살펴보려면 에 대한 액세스 관리 AWS DataSync 섹션을 참조하십시오.

주제

- 에 대한 액세스 관리 AWS DataSync
- AWS 에 대한 관리형 정책 AWS DataSync
- 에 대한 IAM 고객 관리형 정책 AWS DataSync
- DataSync에 서비스 연결 역할 사용
- 생성 중 DataSync 리소스에 태그를 지정하는 권한
- 교차 서비스 혼동된 대리인 방지

에 대한 액세스 관리 AWS DataSync

모든 AWS 리소스는에서 소유합니다 AWS 계정. 리소스를 생성하고 액세스할 수 있는 권한은 권한 정책에서 관리합니다. 계정 관리자는 AWS Identity and Access Management (IAM) 자격 증명에 권한 정책을 연결할 수 있습니다. 일부 서비스(예: AWS Lambda)는 리소스에 권한 정책 연결도 지원합니다.

> **Note**
>
> 계정 관리자는 AWS 계정에 대한 관리자 권한을 가진 사용자입니다. 자세한 내용은 IAM 사용 설명서의 IAM 모범 사례를 참조하십시오.

주제

- DataSync 리소스 및 작업
- 리소스 소유권 이해
- 리소스 액세스 관리
- 정책 요소 지정: 작업, 효과, 리소스, 보안 주체
- 정책에서 조건 지정
- VPC 엔드포인트 정책 생성

DataSync 리소스 및 작업

DataSync에서 기본 리소스는 에이전트, 위치, 작업 및 작업 실행입니다.

다음 표에서처럼 이러한 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연계됩니다.

리소스 유형	ARN 형식
에이전트 ARN	`arn:aws:datasync:region:account-id:agent/agent-id`
위치 ARN	`arn:aws:datasync:region:account-id:location/location-id`
작업 ARN	`arn:aws:datasync:region:account-id:task/task-id`
작업 실행 ARN	`arn:aws:datasync:region:account-id:task/task-id/execution/exec-id`

작업 생성과 같은 특정 API 작업에 대한 권한을 부여하기 위해 DataSync는 권한 정책에서 지정할 수 있는 일련의 작업을 정의합니다. API 작업에는 둘 이상의 작업에 대한 권한이 필요할 수 있습니다.

리소스 소유권 이해

리소스 소유자는 리소스를 AWS 계정 생성한 입니다. 즉, 리소스 소유자는 리소스를 생성하는 요청을 인증하는 보안 주체 엔터티(예: IAM 역할) AWS 계정 의 입니다. 다음 예에서는 이 행동의 작용 방식을 설명합니다.

- 의 루트 계정 자격 증명을 사용하여 작업을 AWS 계정 생성하는 경우 AWS 계정 는 리소스의 소유자입니다(DataSync에서 리소스는 작업임).
- 에서 IAM 역할을 생성하고 해당 사용자에게 `CreateTask` 작업에 대한 권한을 AWS 계정 부여하는 경우 사용자는 작업을 생성할 수 있습니다. 하지만 해당 사용자가 속한 자신의 AWS 계정이 작업 리소스를 소유합니다.
- 작업을 생성할 권한이 AWS 계정 있는에서 IAM 역할을 생성하는 경우 해당 역할을 수임할 수 있는 사람은 누구나 작업을 생성할 수 있습니다. 역할 AWS 계정이 속한이 작업 리소스를 소유합니다.

리소스 액세스 관리

권한 정책은 누가 무엇에 액세스 할 수 있는지를 나타냅니다. 다음 섹션에서는 권한 정책을 만드는 데 사용 가능한 옵션에 대해 설명합니다.

> **Note**
>
> 이 섹션에서는 DataSync의 맥락에서의 IAM을 사용을 논의합니다. IAM 서비스에 대한 자세한 내용은 다루지 않습니다. IAM 설명서 전체 내용은 IAM 사용 설명서의 IAM이란 무엇입니까?

단원을 참조하십시오. IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS Identity and Access Management 정책 참조 섹션을 참조하십시오.

IAM 보안 인증에 연결된 정책을 보안 인증 기반 정책(IAM 정책)이라 하고, 리소스에 연결된 정책을 리소스 기반 정책이라고 합니다. DataSync는 보안 인증 기반 정책(IAM 정책)만 지원합니다.

주제

- 보안 인증 기반 정책
- 리소스 기반 정책

보안 인증 기반 정책

IAM 정책을 사용하여 DataSync 리소스 액세스를 관리할 수 있습니다. 이러한 정책은 AWS 계정 관리자가 DataSync를 사용하여 다음을 수행하는 데 도움이 될 수 있습니다.

- DataSync 리소스를 생성하고 관리할 수 있는 권한 부여 -의 IAM 역할이 에이전트, 위치 및 작업과 같은 DataSync 리소스를 생성하고 관리할 AWS 계정 수 있도록 허용하는 IAM 정책을 생성합니다.
- 다른 AWS 계정 또는의 역할에 권한 부여 AWS 서비스 - 다른 AWS 계정 또는의 IAM 역할에 권한을 부여하는 IAM 정책을 생성합니다 AWS 서비스. 예제:
  1. 계정 A 관리자는 IAM 역할을 생성하고 계정 A의 리소스에 대한 권한을 부여하는 역할에 권한 정책을 연결합니다.
  2. 계정 A 관리자는 계정 B를 역할을 수임할 보안 주체로 식별하는 역할에 신뢰 정책을 연결합니다.

     역할을 수임할 수 있는 AWS 서비스 권한을 부여하기 위해 계정 A 관리자는 신뢰 정책의 보안 주체 AWS 서비스 로를 지정할 수 있습니다.
  3. 그런 다음 계정 B 관리자는 계정 B의 모든 사용자에게 역할을 맡을 수 있는 권한을 위임할 수 있습니다. 이렇게 하면 계정 B에서 역할을 사용하는 모든 사용자가 계정 A에서 리소스를 만들거나 액세스할 수 있습니다.

  IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 액세스 관리 단원을 참조하십시오.

다음은 모든 리소스의 모든 `List*`작업에 대한 권한을 부여하는 정책의 예시입니다. 이 작업은 읽기 전용 작업이며 리소스 수정이 허용되지 않습니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllListActionsOnAllResources",
            "Effect": "Allow",
            "Action": [
                "datasync:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

DataSync에서 보안 인증 기반 정책을 사용하는 방법에 대한 자세한 내용은 관리형 정책 및 고객 AWS 관리형 정책을 참조하세요. IAM에 대한 일반적인 내용은 IAM 사용 설명서를 참조하십시오.

리소스 기반 정책

Amazon S3과 같은 다른 서비스는 리소스 기반 권한 정책을 지원합니다. 예를 들어 Amazon S3 버킷에 정책을 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. 그러나 DataSync는 리소스 기반 정책을 지원하지 않습니다.

정책 요소 지정: 작업, 효과, 리소스, 보안 주체

각 DataSync 리소스에 대해, 해당 서비스는 API 작업 세트를 정의합니다(작업 참조). 이러한 API 작업에 대한 권한을 부여하기 위해 DataSync는 귀하가 정책에서 지정할 수 있는 작업을 정의합니다. 예를 들어 `CreateTask` DataSync 리소스에 대해 `DeleteTask` 및 `DescribeTask`작업을 정의합니다. API 작업을 실시하려면 둘 이상의 작업에 대한 권한이 필요할 수 있습니다.

다음은 가장 기본적인 정책 요소입니다.

- 리소스 – 정책에서 Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다. DataSync 리소스의 경우에는(`*`) IAM 정책에 와일드카드 문자를 사용할 수 있습니다. 자세한 설명은 DataSync 리소스 및 작업섹션을 참조하세요.
- 작업 – 작업 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다. 예를 들면, 지정된 `Effect`요소에 따라 `datasync:CreateTask`권한은 DataSync `CreateTask`작업을 수행할 수 있는 사용자 권한을 허용하거나 거부합니다.

- 결과 – 사용자가 특정 작업을 요청하는 경우의 결과를 귀하가 지정합니다. 이는 `Allow`또는 `Deny`중에 하나가 될 수 있습니다. 리소스에 대한 액세스 (`Allow`) 권한을 명시적으로 부여하지 않으면 액세스가 묵시적으로 거부됩니다. 다른 정책에서 액세스 권한을 부여하는 경우라도 귀하는 사용자가 해당 리소스에 액세스할 수 없도록 하기 위해 리소스에 대한 사용자 액세스 권한을 명시적으로 거부할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 권한 부여를 참조하십시오.
- 보안 주체 – 보안 인증 기반 정책(IAM 정책)에서 정책이 연결되는 사용자는 암시적인 보안 주체입니다. 리소스 기반 정책의 경우, 사용자, 계정, 서비스 또는 권한의 수신자인 기타 개체를 지정합니다 (리소스 기반 정책에만 해당). DataSync는 리소스 기반 정책을 지원하지 않습니다.

IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS Identity and Access Management 정책 참조를 참조하십시오.

정책에서 조건 지정

권한을 부여할 때 IAM 정책 언어를 사용하여 정책이 적용되는 조건을 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어에서의 조건 지정에 관한 자세한 내용은 IAM 사용 설명서의 조건을 참조하십시오.

조건을 표시하려면 미리 정의된 조건 키를 사용합니다. DataSync에만 해당되는 특정한 조건 키는 없습니다. 그러나 필요에 따라 사용할 수 있는 AWS 광범위한 조건 키가 있습니다. 전체 AWS 와이드 키 목록은 IAM 사용 설명서의 사용 가능한 키를 참조하세요.

VPC 엔드포인트 정책 생성

VPC 엔드포인트 정책은 DataSync VPC 서비스 엔드포인트 및 FIPS 지원 VPC 서비스 엔드포인트를 통해 DataSync API 작업에 대한 액세스를 제어하는 데 도움이 됩니다. VPC 엔드포인트 정책을 사용하면 `CreateTask` 또는 `StartTaskExecution`과 같은 VPC 서비스 엔드포인트를 통해 액세스하는 특정 DataSync API 작업을 제한할 수 있습니다.

엔드포인트 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체.
- 수행할 수 있는 작업
- 작업을 수행할 수 있는 리소스

자세한 정보는 엔드포인트 정책을 사용하여 VPC 엔드포인트에 대한 액세스 제어를 참조하세요.

예제 정책

다음은 엔드포인트 정책의 예입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
          "datasync:CreateTask",
          "datasync:StartTaskExecution",
          "datasync:DescribeTask"
        ],
        "Resource": "arn:aws:datasync:us-east-1:123456789012:task/*"
      }
   ]
}
```

AWS 에 대한 관리형 정책 AWS DataSync

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 서비스 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 관리ReadOnlyAccess AWS 형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSDataSyncReadOnlyAccess

`AWSDataSyncReadOnlyAccess` 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 DataSync에 대한 읽기 전용 권한을 부여합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 AWSDataSyncReadOnlyAccess를 참조하세요.

AWS 관리형 정책: AWSDataSyncFullAccess

`AWSDataSyncFullAccess` 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 DataSync에 대한 관리 권한을 부여하며 서비스에 AWS Management Console 액세스하는 데 필요합니다.는 DataSync API 작업 및 관련 리소스(예: Amazon S3 버킷, Amazon EFS 파일 시스템, AWS KMS 키 및 Secrets Manager 보안 암호)와 상호 작용하는 작업에 대한 전체 액세스를 `AWSDataSyncFullAccess` 제공합니다. 또한 이 정책은 로그 그룹 생성, 리소스 정책 생성 또는 업데이트를 포함하여 Amazon CloudWatch에 대한 권한을 부여합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 AWSDataSyncFullAccess를 참조하세요.

AWS 관리형 정책: AWSDataSyncServiceRolePolicy

`AWSDataSyncServiceRolePolicy` 정책을 IAM 자격 증명에 연결할 수 없습니다. 이 정책은 서비스 연결 역할에 연결되어 DataSync에서 사용자를 대신하여 작업을 수행하도록 허용합니다. 자세한 내용은 DataSync에 서비스 연결 역할 사용 단원을 참조하십시오.

이 정책은 관리 권한을 부여하여 서비스 연결 역할이 확장 모드를 사용하여 DataSync 작업에 대한 Amazon CloudWatch Logs를 생성하도록 허용합니다.

정책 업데이트

변경	설명	Date
AWSDataSyncFullAccess - 변경 사항	DataSync가 `AWSDataSyncFullAccess` 에 대한 권한 문을 다음과 같이 수정했습니다. 업데이트된 문은 DataSync가 Secrets Manager 보안 암호 생성 시 사용하는 권한에서 태그 지정 조건을 제거하였습니다.	2025년 5월 13일

변경	설명	Date
AWSDataSyncFullAccess - 변경 사항	DataSync는 AWSDataSyncFullAccess 에 새로운 권한을 추가했습니다. • secretsmanager:CreateSecret • secretsmanager:PutSecretValue • secretsmanager:DeleteSecret • secretsmanager:UpdateSecret 이러한 권한에 따라 DataSync는 AWS Secrets Manager 보안 암호를 생성, 편집, 삭제할 수 있습니다.	2025년 5월 7일
AWSDataSyncFullAccess - 변경 사항	DataSync는 AWSDataSyncFullAccess 에 새로운 권한을 추가했습니다. • secretsmanager:ListSecrets • kms:ListAliases • kms:DescribeKey 이러한 권한을 통해 DataSync는 AWS KMS 키와 연결된 별칭을 AWS Secrets Manager 포함하여 보안 암호 및 키에 대한 메타데이터를 검색할 수 있습니다.	2025년 4월 23일

변경	설명	Date
AWSDataSyncServiceRolePolicy - 변경 사항	DataSync는 DataSync 서비스 연결 역할 `AWSServiceRoleForDataSync` 에서 사용하는 `AWSDataSyncServiceRolePolicy` 정책에 새 권한을 추가했습니다. • `secretsmanager:DescribeSecret` • `secretsmanager:GetSecretValue` 이러한 권한을 통해 DataSync는에서 관리하는 보안 암호의 메타데이터와 값을 읽을 수 있습니다 AWS Secrets Manager.	2025년 4월 15일
AWSDataSyncServiceRolePolicy - 새 정책	DataSync는 DataSync 서비스 연결 역할 `AWSServiceRoleForDataSync` 에서 사용하는 정책을 추가했습니다. 이 새로운 관리형 정책은 확장 모드를 사용하는 DataSync 작업에 대해 Amazon CloudWatch Logs를 자동으로 생성합니다.	2024년 10월 30일

변경	설명	Date
AWSDataSyncFullAccess - 변경 사항	DataSync는 AWSDataSyncFullAccess 에 새로운 권한을 추가했습니다. • iam:CreateServiceLinkedRole 이 권한에 따라 DataSync는 사용자를 위한 서비스 연결 역할을 생성할 수 있습니다.	2024년 10월 30일
AWSDataSyncFullAccess - 변경 사항	DataSync는 AWSDataSyncFullAccess 에 새로운 권한을 추가했습니다. • ec2:DescribeRegions 이 권한을 사용하면 AWS 리전 간 전송을 위한 DataSync 작업을 생성할 때 옵트인 리전을 선택할 수 있습니다.	2024년 7월 22일
AWSDataSyncFullAccess - 변경 사항	DataSync는 AWSDataSyncFullAccess 에 새로운 권한을 추가했습니다. • s3:ListBucketVersions 이 권한을 사용하면 DataSync 매니페스트의 특정 버전을 선택할 수 있습니다.	2024년 2월 16일

변경	설명	Date
AWSDataSyncFullAccess - 변경 사항	DataSync는 AWSDataSyncFullAccess 에 새로운 권한을 추가했습니다. • ec2:DescribeVpcEndpoints • elasticfilesystem:DescribeAccessPoints • fsx:DescribeStorageVirtualMachines • outposts:ListOutposts • s3:GetBucketLocation • s3-outposts:ListAccessPoints • s3-outposts:ListRegionalBuckets 이러한 권한은 Amazon EFS, Amazon FSx for NetApp ONTAP, Amazon S3, S3 on Outposts에 대한 DataSync 에이전트 및 위치를 생성하는 데 도움이 됩니다.	2023년 5월 2일
DataSync가 변경 사항 추적 시작	DataSync는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 3월 1일

에 대한 IAM 고객 관리형 정책 AWS DataSync

AWS 관리형 정책 외에도에 대한 자체 자격 증명 기반 정책을 생성하고 이러한 권한이 필요한 AWS Identity and Access Management (IAM) 자격 증명에 AWS DataSync 연결할 수도 있습니다. 이들은 고객 관리형 정책이라 하며, 이는 귀하가 자신의 AWS 계정에서 관리하는 독립형 정책입니다.

> **Important**
>
> 시작하기 전에 DataSync 리소스에 대한 액세스 관리를 위한 기본 개념과 옵션에 대해 알아보는 것이 좋습니다. 자세한 내용은 에 대한 액세스 관리 AWS DataSync 단원을 참조하십시오.

고객 관리형 정책을 생성할 때 특정 AWS 리소스에서 사용할 수 있는 DataSync 작업에 대한 문을 포함합니다. 다음 정책 예제에는 두 개의 진술이 있습니다(각 진술 내 `Action`및 `Resource`요소에 주목).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllTasks",
            "Effect": "Allow",
            "Action": "datasync:DescribeTask",
            "Resource": "arn:aws:datasync:us-east-1:111122223333:task/*"
        },
        {
            "Sid": "ListAllTasks",
            "Effect": "Allow",
            "Action": "datasync:ListTasks",
            "Resource": "*"
        }
    ]
}
```

정책의 진술은 다음을 수행합니다.

- 첫 번째 진술은 Amazon 리소스 이름(ARN)을 와일드카드 문자(*)로 지정하여 특정 전송 작업 리소스에서 `datasync:DescribeTask`작업을 수행할 권한을 부여합니다.

- 두 번째 진술은 와일드카드 문자(*)만 지정하여 모든 작업에 대해 datasync:ListTasks작업을 수행할 권한을 부여합니다.

고객 관리형 정책에 대한 예제입니다.

다음은 다양한 DataSync 작업에 대한 권한을 부여하는 고객 관리형 정책의 예입니다. 정책은 AWS Command Line Interface (AWS CLI) 또는 AWS SDK를 사용하는 경우 작동합니다. 콘솔에서 이러한 정책을 사용하려면 관리형 정책AWSDataSyncFullAccess도 사용해야 합니다.

주제

- 예제 1: DataSync가 Amazon S3버킷에 액세스할 수 있도록 허용하는 신뢰 관계 생성
- 예제 2: DataSync가 Amazon S3 버킷에 읽기 및 쓰기를 할 수 있도록 허용
- 예제 3: DataSync가 CloudWatch 로그 그룹에 로그를 업로드하도록 허용

예제 1: DataSync가 Amazon S3버킷에 액세스할 수 있도록 허용하는 신뢰 관계 생성

다음은 DataSync가 IAM 역할을 담당하도록 허용하는 신뢰 정책의 예입니다. 이 역할을 통해 DataSync는 Amazon S3 버킷에 액세스할 수 있습니다. 서비스 간 혼동되는 대리인 문제를 방지하려면 정책에서 aws:SourceArn및 aws:SourceAccount글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다.

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:*"
                }
```

```
            }
        }
    ]
}
```

예제 2: DataSync가 Amazon S3 버킷에 읽기 및 쓰기를 할 수 있도록 허용

다음 예제 정책은 DataSync에 대상 위치로 사용되는 S3 버킷에 데이터를 읽고 쓸 수 있는 최소 권한을 부여합니다.

> **Note**
>
> `aws:ResourceAccount`의 값은 정책에 명시된 Amazon S3 버킷을 소유한 계정의 ID여야 합니다.

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

예제 3: DataSync가 CloudWatch 로그 그룹에 로그를 업로드하도록 허용

DataSync는 로그를 Amazon CloudWatch Logs 그룹에 업로드할 수 있는 권한을 요구합니다. CloudWatch 로그 그룹을 사용하면 작업을 모니터링하고 디버깅할 수 있습니다.

이러한 권한을 부여하는 IAM 정책의 예는 DataSync가 CloudWatch 로그 그룹에 로그를 업로드하도록 허용섹션을 참조하십시오.

DataSync에 서비스 연결 역할 사용

AWS DataSync 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 DataSync에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 DataSync에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

주제

- DataSync에 역할 사용

DataSync에 역할 사용

AWS DataSync 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 DataSync에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 DataSync에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 DataSync를 더 쉽게 설정할 수 있습니다. DataSync에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, DataSync만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 DataSync 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

DataSync에 대한 서비스 연결 역할 권한

DataSync는 AWSServiceRoleForDataSync라는 서비스 연결 역할을 사용합니다. DataSync는에서 보안 암호 읽기 AWS Secrets Manager, CloudWatch 로그 그룹 및 이벤트 생성 등 전송 작업 실행에 필요한 작업을 수행할 수 있습니다.

AWSServiceRoleForDataSync 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `datasync.amazonaws.com`

서비스 연결 역할은 AWSDataSyncServiceRolePolicy라는 AWS 관리형 정책을 사용하며, 이를 통해 DataSync는 지정된 리소스에서 다음 작업을 완료할 수 있습니다.

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}"
                }
            }
        }
    ]
}
```

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

DataSyn 에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 DataSync 작업을 생성하면 DataSync가 서비스 연결 역할을 생성합니다.

AWS CLI 또는 AWS API에서 서비스 이름으로 `datasync.amazonaws.com` 서비스 연결 역할을 생성할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 서비스 연결 역할 생성 섹션을 참조하세요. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. DataSync 작업을 생성할 때 DataSync는 사용자를 위해 서비스 연결 역할을 다시 생성합니다.

이 서비스 연결 역할을 삭제한 후 동일한 IAM 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

DataSync에 대한 서비스 연결 역할 편집

DataSync는 AWSServiceRoleForDataSync 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

DataSync에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할을 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할을 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다.

> **Note**
>
> 리소스를 삭제하려 할 때 DataSync 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForDataSync에서 사용하는 DataSync 리소스를 삭제하는 방법

1. 작업에서 사용하는 DataSync 에이전트를 삭제합니다(있는 경우).
2. 작업의 위치를 삭제합니다.
3. 작업을 삭제합니다.

수동으로 서비스 연결 역할 삭제

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForDataSync 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

DataSync 서비스 연결 역할이 지원되는 리전

DataSync는 서비스를 사용할 수 있는 모든 리전에 서비스 연결 역할을 사용하도록 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 단원을 참조하세요.

생성 중 DataSync 리소스에 태그를 지정하는 권한

일부 리소스 생성 AWS DataSync API 작업을 사용하면 리소스를 생성할 때 태그를 지정할 수 있습니다. 리소스 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 구현할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 ABAC란 무엇입니까 AWS?를 참조하세요.

사용자가 생성 시 리소스에 태그를 지정할 수 있으려면 리소스를 생성하는 작업을 사용할 권한이 있어야 합니다(예: `datasync:CreateAgent`또는 `datasync:CreateTask`). 리소스 생성 작업에서 태그가 지정되면 사용자는 `datasync:TagResource`작업을 사용할 명시적 권한도 가지고 있어야 합니다.

`datasync:TagResource` 작업은 리소스 생성 작업 도중 태그가 적용되는 경우에만 평가됩니다. 따라서 리소스를 생성할 권한이 있는 사용자(태그 지정 조건은 없다고 가정)는 요청에서 태그가 지정되지 않은 경우, `datasync:TagResource`작업을 사용할 권한이 필요하지 않습니다.

하지만 사용자가 태그를 사용하여 리소스 생성을 시도하는 경우, 사용자에게 `datasync:TagResource`작업을 사용할 권한이 없다면 요청은 실패합니다.

IAM 정책 진술의 예제

다음 예제 IAM 정책 문을 사용하여 DataSync 리소스를 생성하는 사용자에게 `TagResource`권한을 부여합니다.

다음 명령문을 사용하면 에이전트를 생성할 때 DataSync 에이전트에 태그를 지정할 수 있습니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:444455556666:agent/*"
        }
    ]
```

```
}
```

다음 명령문을 사용하면 위치를 생성할 때 DataSync 위치에 태그를 지정할 수 있습니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:111122223333:location/*"
        }
    ]
}
```

다음 명령문을 사용하면 사용자가 작업을 생성할 때 DataSync 작업에 태그를 지정할 수 있습니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:444455556666:task/*"
        }
    ]
}
```

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS교차 서비스 가장은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(직접 호출하는 서비스)가 다른 서비스(직접 호출되는 서비스)

를 직접 호출할 때 발생할 수 있습니다. 직접 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 위탁자를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에서 aws:SourceArn 및 aws:SourceAccount 전역 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스를 AWS DataSync 제공하는 권한을 제한하는 것이 좋습니다. 두 전역 조건 컨텍스트 키와 계정을 포함한 aws:SourceArn 값을 모두 사용하는 경우, aws:SourceAccount 값 및 aws:SourceArn 값의 계정은 동일한 정책 명령문에서 사용할 경우 반드시 동일한 계정 ID를 사용해야 합니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 aws:SourceArn을 사용하세요. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 하려면 aws:SourceAccount를 사용하세요.

aws:SourceArn의 값에는 DataSync가 IAM 역할을 수임할 수 있도록 허용되는 DataSync 위치 ARN이 포함되어야 합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 aws:SourceArn 키를 사용하는 것입니다. 전체 ARN을 모르거나 여러 리소스를 지정하는 경우, 알 수 없는 부분에 대해 와일드카드 문자(*)를 사용합니다. 다음은 DataSync에서 사용하는 방법의 예입니다.

- 신뢰 정책을 기존 DataSync 위치로 제한하려면 정책에 전체 위치 ARN을 포함합니다. DataSync는 특정 위치를 처리할 때만 IAM 역할을 맡습니다.
- DataSync용 Amazon S3 위치를 생성할 때는 해당 위치의 ARN을 알 수 없습니다. 이러한 시나리오에서는 aws:SourceArn키에 다음 형식을 사용하세요: arn:aws:datasync:*us-east-2*:*123456789012*:*. 이 형식은 파티션(aws), 계정 ID 및 리전의 유효성을 검사합니다.

다음 전체 예는 신뢰 정책에 aws:SourceArn및 aws:SourceAccount전역 조건 컨텍스트 키를 DataSync와 함께 사용하여 혼동된 대리인 문제를 방지하는 방법을 보여줍니다.

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:*"
                }
            }
        }
    ]
}
```

aws:SourceArn 및 aws:SourceAccount전역 조건 컨텍스트 키를 DataSync와 함께 사용하는 방법을 보여주는 추가 예는 다음 주제를 참조하세요.

- DataSync가 사용자 Amazon S3 버킷에 액세스할 수 있도록 허용하는 신뢰 관계 생성
- Amazon S3 버킷에 액세스할 IAM 역할을 구성합니다

의 규정 준수 검증AWS DataSync

AWS 서비스가 특정 규정 준수 프로그램의 범위에 포함되는지 알아보려면 규정 준수 프로그램 제공 범위 내 AWS 서비스를 참조하고 관심 있는 규정 준수 프로그램을 선택하십시오. 일반적인 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact(을)를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact에서 보고서 다운로드를 참조하세요.

AWS 서비스 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 결정됩니다. AWS 서비스 사용 시 규정 준수 책임에 대한 자세한 내용은 AWS 보안 설명서를 참조하세요.

AWS DataSync의 복원성

AWS 글로벌 인프라는 AWS리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 다수의 가용 리전을 제공하며 이러한 가용 리전은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

> **Note**
>
> DataSync 작업을 실행 중 데이터를 마이그레이션하는 가용 영역이 실패하면 작업 역시 실패합니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하십시오.

AWS DataSync에서 인프라 보안

관리형 서비스인 AWSDataSync는 AWS글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 DataSync에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

Secrets Manager를 사용하여 스토리지 위치 자격 증명 보호

DataSync는 위치를 사용하여 온프레미스, 다른 클라우드 또는 AWS에 있는 스토리지 리소스에 액세스합니다. 일부 위치 유형에서는 스토리지 시스템으로 인증하기 위해 자격 증명(예: 액세스 키 및 보안 키, 사용자 이름 및 암호, Kerberos 키 탭, SAS 토큰 등)을 제공해야 합니다. 인증에 자격 증명이 필요한 DataSync 위치를 생성할 때 AWS Secrets Manager (Secrets Manager)를 사용하여 자격 증명의 보안 암호를 저장할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

- ManagedSecretConfig: DataSync 관리형 보안 암호 구성. 기본 키로 암호화된 DataSync 서비스 관리형 보안 암호를 사용하여 Secrets Manager에 보안 암호를 저장합니다.
- CmkSecretConfig: 고객 관리형 키(CMK) 구성을 사용하는 DataSync 관리형 보안 암호입니다. 관리하는 AWS KMS 키로 암호화된 DataSync 서비스 관리형 보안 암호를 사용하여 Secrets Manager에 보안 암호를 저장합니다.

- CustomSecretConfig: 고객 관리형 보안 암호 구성. 생성 및 관리하는 보안 암호와 키를 사용하여 보안 암호를 Secrets Manager에 저장합니다. DataSync는 사용자가 제공한 IAM 역할을 사용하여 이 보안 암호에 액세스합니다.

Secrets Manager 보안 암호는 모든 경우에 사용자의 계정에 저장되므로, 필요에 따라 DataSync 서비스와 독립적으로 보안 암호를 업데이트할 수 있습니다. DataSync에서 생성하고 관리하는 보안 암호에는 `aws-datasync` 접두사가 있습니다.

DataSync 외부에서 보안 암호를 생성하거나 DataSync 이외의 서비스에서 서비스 관리형 보안 암호에 대한 API 호출을 수행하는 경우에만 보안 암호 사용에 대한 요금이 부과됩니다.

기본 키로 암호화된 서비스 관리형 보안 암호 사용

DataSync 위치 생성 시 사용자는 보안 암호 문자열만 제공합니다. DataSync는 Secrets Manager에 보안 암호 리소스를 생성하여 사용자가 제공한 보안 암호를 저장하고 계정의 기본 Secrets Manager KMS 키로 보안 암호를 암호화합니다. Secrets Manager에서 직접 보안 암호 값을 변경하거나 DataSync 콘솔 AWS CLI또는 SDK를 사용하여 위치를 업데이트하여 보안 암호 값을 변경할 수 있습니다. 위치 리소스를 삭제하거나 사용자 지정 보안 암호를 사용하도록 업데이트하면 DataSync가 보안 암호 리소스를 자동으로 삭제합니다.

> **Note**
>
> Secrets Manager에서 보안 암호 리소스를 생성, 수정, 삭제하려면 DataSync에 적절한 권한이 있어야 합니다. 자세한 내용은 DataSync에 대한AWS 관리형 정책을 참조하세요.

사용자 지정 AWS KMS 키로 암호화된 서비스 관리형 보안 암호 사용

DataSync 위치 생성 시 사용자는 AWS KMS 키의 보안 암호와 ARN을 제공합니다. DataSync는 Secrets Manager에 보안 암호 리소스를 자동으로 생성하여 사용자가 제공한 보안 암호를 저장하고 AWS KMS 키를 사용하여 암호화합니다. Secrets Manager에서 직접 또는 DataSync 콘솔 또는 AWS CLI SDK를 사용하여 위치를 업데이트하여 보안 암호 값을 변경할 수 있습니다. 위치 리소스를 삭제하거나 사용자 지정 보안 암호를 사용하도록 업데이트하면 DataSync가 보안 암호 리소스를 자동으로 삭제합니다.

> **Note**
>
> AWS KMS 키는 ENCRYPT_DECRYPT 키 유형과 함께 대칭 암호화를 사용해야 합니다. 자세한 내용은 AWS Secrets Manager 사용 설명서의 AWS Key Management Service 키 선택을 참조하세요.

Secrets Manager에서 보안 암호 리소스를 생성, 수정, 삭제하려면 DataSync에 적절한 권한이 있어야 합니다. 자세한 내용은 AWS 관리형 정책AWSDataSyncFullAccess 단원을 참조하십시오.

올바른 DataSync 관리형 정책을 사용할 뿐만 아니라, 다음 권한도 갖추어야 합니다.

```
{
    "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*을 KMS 키 ARN으로 변경합니다.

보안 암호 값을 검색하고 해독하기 위해 DataSync는 서비스 연결 역할(SLR)을 사용하여 AWS KMS 키에 액세스합니다. DataSync가 KMS 키를 사용하도록 하려면 키의 정책 설명에 다음을 추가합니다.

```
{
    "Sid": "Allow DataSync to use the key for decryption",
    "Effect": "Allow",
    "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync"
    },
    "Action": "kms:Decrypt",
```

```
    "Resource": "*"
}
```

*111122223333*을 AWS 계정 ID로 바꿉니다.

사용자가 관리하는 보안 암호 사용

DataSync 위치를 생성하기 전에 Secrets Manager에서 보안 암호를 생성합니다. 보안 암호 값은 보안 암호 문자열만 일반 텍스트로 포함해야 합니다. DataSync 위치를 생성할 때 보안 암호의 ARN과 DataSync가 보안 암호와 보안 암호를 암호화하는 데 사용되는 AWS KMS 키 모두에 액세스하는 데 사용하는 IAM 역할을 제공합니다. 적절한 권한이 있는 IAM 역할을 생성하려면 다음을 수행합니다.

1. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
2. 왼쪽 탐색 창의 액세스 관리에서 역할을 선택한 다음, 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택 페이지의 신뢰할 수 있는 엔터티 유형에서 AWS 서비스를 선택합니다.
4. 사용 사례를 확인하려면 드롭다운 목록에서 DataSync를 선택합니다. 다음을 선택합니다.
5. 권한 추가 페이지에서 다음을 선택합니다. 역할의 이름을 입력한 후 역할 생성을 선택합니다.
6. 역할 페이지에서 방금 생성한 역할의 이름을 검색해 선택합니다.
7. 역할의 세부 정보 페이지에서 권한 탭을 선택합니다. 권한 추가를 선택한 후 인라인 정책 생성을 선택합니다.
8. JSON 탭을 선택한 후 다음 권한을 정책 편집기에 추가합니다.

   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"
        }
    ]
```

```
}
```

Secrets Manager 보안 암호의 이름을 *your-secret-name*으로 변경합니다.

9. 다음을 선택합니다. 정책 이름을 입력하고 정책 생서을 선택합니다.
10. (권장) 교차 서비스 혼동된 대리자 문제를 방지하려면 다음을 수행합니다.

    a. 역할의 세부 정보 페이지에서 신뢰 관계 탭을 선택합니다. 신뢰 정책 편집을 선택합니다.

    b. `aws:SourceArn` 및 `aws:SourceAccount`전역 조건 컨텍스트 키가 포함된 다음 예를 사용하여 신뢰 정책을 업데이트하세요.

    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. 정책 업데이트를 선택합니다.

위치를 생성할 때 이 역할을 지정할 수 있습니다. 보안 암호가 암호화에 고객 관리형 AWS KMS 키를 사용하는 경우 이전 절차에서 생성한 역할에서 액세스를 허용하도록 키의 정책도 업데이트해야 합니다. 정책을 업데이트하려면 AWS KMS 키의 정책 설명에 다음을 추가합니다.

```
{
    "Sid": "Allow DataSync use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam:111122223333:role/your-role-name”
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

*111122223333*을 AWS 계정 ID로 바꾸고 *your-role-name*을 이전 절차에서 생성한 IAM 역할의 이름으로 바꿉니다.

> **Note**
>
> Secrets Manager에 암호를 저장하면 AWS 계정 에 요금이 발생합니다. 요금에 대한 자세한 내용은 AWS Secrets Manager 요금을 참조하십시오.

AWS DataSync 할당량

AWS DataSync로 작업할 때의 리소스 할당량 및 한도를 알아봅니다.

스토리지 시스템, 파일, 객체 제한

다음 표에는 DataSync가 스토리지 시스템, 파일 및 객체를 사용할 때 적용되는 제한 사항이 설명되어 있습니다.

설명	Limit
총 파일 경로 최대 길이	4,096바이트
파일 경로 구성 요소(파일 이름, 디렉터리 또는 서브디렉터리) 최대 길이	255바이트
윈도우 도메인의 최대 길이	253자
서버 호스트 이름 최대 길이	255자
Amazon S3 객체 이름 최대 길이	1,024자(UTF-8)

DataSync 할당량

다음 표에서는 특정 AWS 계정 및 리전에서의 DataSync 리소스 할당량을 설명합니다.

리소스	할당량	조정 가능
생성할 수 있는 최대 작업 수	100	예
(확장 모드 작업) DataSync가 작업 실행당 처리할 수 있는 최대 소스 및 대상 객체 수 자세한 내용은 DataSync가 파일, 객체, 디렉터리를 전송하는 방법 섹션을 참조하세요.	사실상 무제한	N/A
(기본 모드 작업) 온프레미스, 자체 관리형, 다른 클라우드 스토리지 및 AWS 스토리지 서비스 간	5천만	예

리소스	할당량	조정 가능
의 작업 실행당 DataSync가 작업할 수 있는 최대 소스 및 대상 파일, 객체, 디렉터리 수 자세한 내용은 DataSync가 파일, 객체, 디렉터리를 전송하는 방법 섹션을 참조하세요.	**Important** 이 할당량에 대해 다음 사항을 기억하세요. • 접두사가 있는 Amazon S3 객체를 전송하는 경우 접두사는 디렉터리로 취급되며 할당량에 포함됩니다. 예를 들어 DataSync는 `s3://bucket/foo/bar.txt` 를 두 개의 디렉터리(`./` 및 `./foo/`)와 하나의 객체(`bar.txt`)로 간주합니다. • 2천만 개가 넘는 파일, 개체 또는 디렉터리로 작업하는 작업의 경우 DataSync 에이전트에 최소 64GB의 RAM을 할당해야 합니다. 자세한 내용은 DataSync 이전에 대한 에이전트 요구 사항을 참조하세요.	**Tip** 증가를 요청하는 대신 포함 및 제외 필터를 사용하여 특정 디렉터리에 초점을 맞추는 작업을 생성할 수 있습니다. 자세한 내용과 예제는 DataSync에서 전송된 데이터 필터

리소스	할당량	조정 가능
		링을 참조하세요.

리소스	할당량	조정 가능
(기본 모드 작업) AWS 스토리지 서비스 간의 작업 실행당 DataSync가 작업할 수 있는 최대 소스 및 대상 파일, 객체, 디렉터리 수 자세한 내용은 DataSync가 파일, 객체, 디렉터리를 전송하는 방법 섹션을 참조하세요.	2천5백만 개 **Important** 접두사가 있는 Amazon S3 객체를 전송하는 경우 접두사는 디렉터리로 취급되며 할당량에 포함됩니다. 예를 들어 DataSync는 `s3://bucket/foo/bar.txt` 를 두 개의 디렉터리(`./` 및 `./foo/`)와 하나의 객체(`bar.txt`)로 간주합니다.	예 **Tip** 증가를 요청하는 대신 포함 및 제외 필터를 사용하여 특정 디렉터리에 초점을 맞추는 작업을 생성할 수 있습니다. 자세한 내용과 예제는 DataSync에서 전송된 데

리소스	할당량	조정 가능
		이터 필터 링을 참조 하세 요.
작업당 최대 처리량(DataSync 에이전트를 사용하는 전송의 경우)	10Gbps	아니요
작업당 최대 처리량(DataSync 에이전트를 사용하지 않는 전송의 경우)	5Gbps	아니요
작업 필터에 포함할 수 있는 최대 문자 수	102,400자 **Note** DataSync 콘솔을 사용하는 경우 이 제한에는 포함 및 제외 패턴에 결합된 모든 문자가 포함됩니다.	아니요
단일 작업에 대해 대기열에 있는 최대 실행 수	50	아니요
확장 모드 작업의 최대 동시 실행 수	120	아니요
작업 실행 내역이 보관되는 최대 일수	30	아니요
확장 모드 작업에서 매니페스트 파일의 최대 크기	20GB	아니요

할당량 증가 요청

사용자는 DataSync 할당량을 높이도록 요청할 수 있습니다. 증가는 즉시 승인되지 않으며 적용되기까지 며칠이 걸릴 수 있습니다.

할당량 증가 요청

1. https://console.aws.amazon.com/servicequotas/에서 Service Quotas 콘솔을 엽니다.
2. 탐색 창에서 AWS 서비스를 선택한 다음 AWS DataSync를 선택합니다.
3. 늘리려는 할당량을 선택한 다음 계정 수준에서 증가 요청을 선택합니다.
4. 원하는 할당량 총량을 입력한 다음 요청을 선택합니다.

   할당량을 다르게 늘려야 하는 경우 별도의 요청을 작성하세요.

AWS DataSync 문제 해결

다음 정보를 사용하여 AWS DataSync 문제 및 오류를 해결합니다.

주제

- DataSync 에이전트 관련 문제 해결
- DataSync 위치 관련 문제 해결
- DataSync 작업 관련 문제 해결
- 데이터 확인 문제 해결
- DataSync를 사용한 예상보다 높은 S3 스토리지 비용 문제 해결

DataSync 에이전트 관련 문제 해결

다음 정보를 사용하여 AWS DataSync 에이전트 관련 문제를 해결할 수 있습니다. 이러한 문제에는 다음이 포함될 수 있습니다.

- Amazon EC2 에이전트의 로컬 콘솔 연결 문제
- 에이전트의 활성화 키 검색 실패
- VPC 서비스 엔드포인트를 사용한 에이전트 활성화 문제
- 에이전트 오프라인 상태 검색

Amazon EC2 에이전트의 로컬 콘솔에 연결하려면 어떻게 해야 합니까?

Amazon EC2 에이전트의 로컬 콘솔에 연결하려면 SSH를 사용해야 합니다. EC2 인스턴스의 보안 그룹이 SSH(TCP 포트 22)를 통한 액세스를 허용하는지 확인합니다.

터미널에서 다음 `ssh`명령을 실행하여 인스턴스에 연결하십시오:

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

- *`/path/key-pair-name`*의 경우 인스턴스에 연결하는 데 필요한 프라이빗 키의 경로와 파일 이름(`.pem`)을 지정합니다.
- *`instance-user-name`*의 경우 `admin`를 지정합니다.

- *instance-public-ip-address*의 경우, 인스턴스의 퍼블릭 IP 주소를 지정합니다.

에이전트 활성화 키 검색 실패 오류는 무엇을 의미하나요?

DataSync 에이전트를 활성화할 때 에이전트는 활성화 키를 요청하기 위해 지정한 서비스 엔드포인트에 연결됩니다. 이 오류는 네트워크 보안 설정이 연결을 차단하고 있음을 의미할 수 있습니다.

취할 조치

Virtual Private Cloud(VPC) 서비스 엔드포인트를 사용하는 경우, 보안 그룹 설정에서 에이전트가 VPC 엔드포인트에 연결할 수 있도록 허용하는지 확인합니다. 필수 포트에 대한 자세한 설명은 VPC 또는 FIPS VPC 서비스 엔드포인트에 대한 네트워크 요구 사항단원을 참조하세요.

퍼블릭 또는 Federal Information Processing Standard(FIPS) 엔드포인트를 사용하는 경우, 방화벽 및 라우터 설정에서 에이전트가 엔드포인트에 연결하도록 허용하는지 확인합니다. 자세한 내용은 퍼블릭 또는 FIPS 서비스 엔드포인트의 네트워크 요구 사항 단원을 참조하세요.

여전히 VPC 서비스 엔드포인트를 사용하여 에이전트를 활성화할 수 없습니다.

VPC 서비스 엔드포인트로 DataSync 에이전트를 활성화하는 데 여전히 문제가 있는 경우 상담원에게 무슨 일이 벌어지고 있는지 모르겠어요. 누군가 저를 도와줄 수 있나요? 섹션을 참조하세요.

에이전트가 오프라인 상태인 경우, 어떻게 해야 하나요?

DataSync 에이전트는 몇 가지 이유로 오프라인 상태일 수 있지만 다시 온라인 상태로 전환할 수 있습니다. 에이전트를 삭제하고 새 에이전트를 생성하기 전에 다음 체크리스트를 검토하여 무슨 일이 발생했는지 파악하세요.

- 백업 팀에 문의 - 스냅샷이나 백업에서 가상 머신(VM)이 복원되어 에이전트가 오프라인 상태인 경우, 에이전트를 교체해야 할 수 있습니다.
- 에이전트의 VM 또는 Amazon EC2 인스턴스가 꺼져 있는지 확인 - 사용 중인 에이전트 타입에 따라 꺼져 있는 경우, VM 또는 EC2 인스턴스를 다시 켜보세요. 다시 켜지면 에이전트의 네트워크 연결을 테스트합니다 AWS.
- 에이전트가 최소 하드웨어 요구 사항을 충족하는지 확인 - 에이전트가 활성화된 이후 VM 또는 EC2 인스턴스 구성이 실수로 변경되어 에이전트가 오프라인 상태일 수 있습니다. 예를 들어 VM에 필요한 최소 메모리 또는 공간이 더 이상 없는 경우, 에이전트는 오프라인으로 표시될 수 있습니다. 자세한 설명은 AWS DataSync 에이전트에 대한 요구 사항섹션을 참조하세요.

- 에이전트 관련 소프트웨어 업데이트가 완료될 때까지 대기 - AWS에서 제공한 소프트웨어 업데이트 이후 에이전트가 잠시 오프라인 상태가 될 수 있습니다. 이것이 에이전트가 오프라인 상태인 이유라고 생각되면 잠시 기다린 다음 에이전트가 다시 온라인 상태인지 확인하세요.
- VPC 서비스 엔드포인트 설정 확인 - 오프라인 에이전트가 공용 서비스 엔드포인트를 사용하고 있고 DataSync용 VPC 서비스 엔드포인트를 생성한 동일한 VPC에서 사용하는 경우, 해당 VPC 엔드포인트에 대한 프라이빗 DNS 지원을 비활성화해야 할 수 있습니다.

이러한 이유 중 어느 것도 에이전트가 오프라인 상태인 것 같지 않으면 에이전트를 교체해야 할 수 있습니다.

상담원에게 무슨 일이 벌어지고 있는지 모르겠어요. 누군가 저를 도와줄 수 있나요?

AWS Support 가 DataSync 에이전트에 액세스하도록 허용하고 에이전트 관련 문제를 해결하는 데 도움을 줄 수 있습니다. 에이전트의 로컬 콘솔을 통해 이 액세스 권한을 활성화해야 합니다.

에이전트에 대한 지원 액세스 권한을 제공하려면

1. 에이전트의 로컬 콘솔에 로그인합니다.
2. 프롬프트에서 **5**를 입력하여 명령 프롬프트를 엽니다(VMware VM의 경우 **6**사용).
3. **h**를 입력하여 AVAILABLE COMMANDS(사용 가능한 명령) 창을 엽니다.
4. 사용 가능한 명령 창에서 다음을 입력해 지원에 연결합니다.

   ```
   open-support-channel
   ```

   VPC 엔드포인트와 함께 에이전트를 사용하는 경우 다음과 같이 지원 채널에 VPC 엔드포인트 IP 주소를 제공해야 합니다.

   ```
   open-support-channel vpc-ip-address
   ```

   AWS에서 지원 채널을 시작하려면 방화벽에서 인바운드 TCP 포트 22를 허용해야 합니다. 에 연결하면 지원 DataSync가 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

   > **Note**
   >
   > 채널 번호는 TCP/UDP 포트 번호가 아닙니다. 그 대신에 서버에 SSH(TCP 22)로 연결하여 해당 연결에 대한 지원 채널을 제공합니다.

5. 지원 채널이 설정되면 문제 해결 지원을 제공할 수 지원 있도록 지원 서비스 번호를에 제공합니다.
6. 지원 세션이 완료되면 **Enter**를 입력하여 세션을 종료합니다.
7. **exit**를 입력하여 DataSync 콘솔에서 로그아웃합니다.
8. 프롬프트 메시지에 따라 로컬 콘솔을 종료합니다.

DataSync 위치 관련 문제 해결

다음 정보를 사용하여 AWS DataSync 위치 관련 문제를 해결할 수 있습니다. 이러한 문제에는 다음이 포함될 수 있습니다.

- NFS 위치의 권한 및 탑재 오류
- 파일 소유권 문제
- Kerberos 인증을 사용하는 SMB 위치 액세스 문제
- Amazon S3 및 Microsoft Azure Blob 위치와 같은 객체 스토리지의 권한 및 액세스 문제

NFS 권한 거부 오류가 발생하여 작업 실패

`root_squash` 또는 `all_squash`로 NFS 파일 서버를 구성하였는데 파일에 읽기 액세스 권한이 부족하면 "권한 거부" 오류 메시지를 받을 수 있습니다.

취할 조치

이 문제를 해결하려면 `no_root_squash`로 NFS 내보내기를 구성하거나 또는 전송하려는 파일 전체를 대상으로 모든 사용자에 대해 읽기 액세스를 허용하는 권한을 부여합니다.

또한 모든 실행 액세스를 활성화해야 DataSync가 디렉터리에 액세스할 수 있습니다. 디렉터리를 탑재할 수 있는지 확인하려면 먼저 에이전트와 동일한 네트워크 구성을 가진 컴퓨터에 연결한 후 이어서 다음 CLI 명령을 실행하십시오:

```
mount -t nfs -o nfsvers=<your-nfs-server-version> <your-nfs-server-
name>:<nfs-export-path-you-specified> <new-test-folder-on-your-computer>
```

그래도 문제가 해결되지 않으면 AWS Support 센터에 문의하세요.

NFS 탑재 오류가 발생하여 작업 실패

NFS 파일 서버 위치와 관련된 DataSync 작업을 실행할 때 다음 오류가 표시될 수 있습니다.

Task failed to access location loc-1111222233334444a: x40016: mount.nfs: Connection timed out

취할 조치

오류가 해결될 때까지 다음 작업을 수행하세요.

1. DataSync 위치에 지정한 NFS 파일 서버와 내보내기가 유효한지 확인합니다. 그렇지 않은 경우 위치 및 작업을 삭제한 다음 유효한 NFS 파일 서버를 사용하여 새 위치 및 작업을 생성하고 내보냅니다. 자세한 내용은 DataSync 콘솔 사용 단원을 참조하십시오.
2. 에이전트와 NFS 파일 서버 간의 방화벽 구성을 확인합니다. 자세한 내용은 온프레미스, 자체 관리형 및 기타 클라우드 스토리지에 대한 네트워크 요구 사항 단원을 참조하십시오.
3. 에이전트가 NFS 파일 서버에 액세스하고 내보내기를 탑재할 수 있는지 확인합니다. 자세한 내용은 DataSync에 NFS 파일 서버 액세스 권한 제공 단원을 참조하십시오.
4. 그래도 오류가 계속 표시되면를 사용하여 지원 채널을 엽니다 지원. 자세한 내용은 상담원에게 무슨 일이 벌어지고 있는지 모르겠어요. 누군가 저를 도와줄 수 있나요? 단원을 참조하십시오.

Amazon EFS 탑재 오류로 작업 실패

Amazon EFS 위치와 관련된 DataSync 작업을 실행할 때 다음과 같은 오류가 발생할 수 있습니다.

Task failed to access location loc-1111222233334444a: x40016: Failed to connect to EFS mount target with IP: 10.10.1.0.

이 문제는 위치로 구성한 Amazon EFS 파일 시스템의 탑재 경로가 업데이트되거나 삭제될 때 발생할 수 있습니다. DataSync는 파일 시스템에서 이러한 변경 사항을 인식하지 못합니다.

취할 조치

위치 및 작업을 삭제하고새 탑재 경로를 사용하여 새 Amazon EFS 위치를 생성합니다.

NFS 전송으로 파일 소유권이 유지되지 않음

전송 후 DataSync 대상 위치의 파일에 소스 위치의 동일한 파일과 다른 사용자 ID(UID) 또는 그룹 ID(GID)가 있음을 알 수 있습니다. 예를 들어 대상의 파일에는 65534, 99 또는 nobody의 UID가 있을 수 있습니다.

전송과 관련된 파일 시스템에서 DataSync가 지원하지 않는 기능인 NFS 버전 4 ID 매핑을 사용하는 경우 발생할 수 있습니다.

취할 조치

이 문제를 해결할 수 있는 몇 가지 옵션이 있습니다.

- NFS 버전 4 대신 버전 3을 사용하는 파일 시스템을 위한 새 위치를 생성합니다.
- 파일 시스템에서 NFS 버전 4 ID 매핑을 비활성화합니다.

전송을 재시도합니다. 두 옵션 중 하나를 수행하면 문제를 해결할 수 있습니다.

작업이 Kerberos를 사용하는 SMB 위치에 액세스할 수 없음

Kerberos 인증을 사용하는 SMB 위치에서 발생하는 DataSync 오류는 일반적으로 위치와 Kerberos 구성 간의 불일치와 관련이 있습니다. 네트워크 문제가 있을 수도 있습니다.

위치 액세스 실패

다음 오류는 SMB 위치 또는 Kerberos 설정에 구성 문제가 있을 수 있음을 나타냅니다.

```
Task failed to access location
```

다음을 확인합니다.

- 위치에 지정한 SMB 파일 서버는 도메인 이름으로 지정됩니다. Kerberos에서는 파일 서버의 IP 주소를 지정할 수 없습니다.
- 위치에 지정하는 Kerberos 보안 주체는 Kerberos 키 테이블(키탭) 파일을 생성하는 데 사용하는 보안 주체와 일치합니다. 보안 주체 이름은 대/소문자를 구분합니다.
- 키탭 파일을 생성한 이후 Kerberos 보안 주체의 매핑된 사용자 암호가 변경되지 않았습니다. (암호 교체 또는 기타 이유로 인해) 암호가 변경되면 다음 오류와 함께 작업 실행이 실패할 수 있습니다.

  Task failed to access location loc-1111222233334444a: x40015: kinit: Preauthentication failed while getting initial credentials

KDC 영역에 연결할 수 없음

다음 오류는 네트워킹 문제를 나타냅니다.

```
kinit: Cannot contact any KDC for realm 'MYDOMAIN.ORG' while getting initial
 credentials"
```

다음을 확인합니다.

- DataSync에 제공한 Kerberos 구성 파일(`krb5.conf`)에는 Kerberos 영역에 대한 올바른 정보가 있습니다. 예시 `krb5.conf` 파일은 Kerberos 인증 사전 조건을 참조하세요.
- Kerberos 키 분배 센터(KDC) 서버 포트가 열려 있습니다. KDC 포트는 일반적으로 TCP 포트 88입니다.
- 네트워크의 DNS 구성입니다.

입력/출력 오류로 작업이 실패했습니다.

스토리지 시스템에서 DataSync 에이전트의 입출력 요청에 장애가 발생하는 경우, 입력/출력 오류 메시지가 표시될 수 있습니다. 일반적인 원인으로는 서버 디스크 장애, 방화벽 구성 변경 또는 네트워크 라우터 장애 등이 있습니다.

NFS 파일 서버 또는 Hadoop 분산 파일 시스템(HDFS) 클러스터와 관련된 오류인 경우 다음 단계를 사용하여 오류를 해결하세요.

취해야 할 조치(NFS)

먼저 NFS 파일 서버의 로그 및 지표를 점검하여 NFS 서버에서 문제가 시작되었는지 확인합니다. 그렇다면 해당 문제를 해결하세요.

그런 다음, 네트워크 구성이 변경되지는 않았는지 확인하세요. NFS 파일 서버가 올바르게 구성되고 DataSync가 액세스할 수 있는지 확인하려면 다음을 수행합니다.

1. 같은 네트워크 서브넷의 다른 NFS 클라이언트를 에이전트로 설정합니다.
2. 해당 클라이언트에 공유를 탑재합니다.
3. 클라이언트가 성공적으로 공유를 읽고 공유에 쓸 수 있는지 확인합니다.

취해야 할 조치(HDFS)

오류를 해결할 때까지 다음 작업을 수행하세요.

1. HDFS 클러스터에서 DataSync 에이전트가 클러스터의 NameNode 및 DataNode 포트와 통신하도록 허용하는지 확인합니다.

   대부분의 클러스터에서는 다음 구성 파일에서 클러스터가 사용하는 포트 번호를 찾을 수 있습니다.

   - NameNode 포트를 찾으려면 `fs.default.name`또는 속성 아래에 있는 `core-site.xml`파일을 살펴보세요(Hadoop `fs.default`배포에 따라 다름).

- DataNode 포트를 찾으려면 `dfs.datanode.address`속성 아래의 `hdfs-site.xml`파일을 살펴보세요.

2. `hdfs-site.xml` 파일에서 `dfs.data.transfer.protection` 속성에 값이 하나만 있는지 확인합니다. 예제:

```
<property>
   <name>dfs.data.transfer.protection</name>
   <value>privacy</value>
</property>
```

오류: `FsS3UnableToConnectToEndpoint`

DataSync는 Amazon S3 위치에 연결할 수 없습니다. 이는 해당 위치의 S3 버킷에 연결할 수 없거나 위치가 올바르게 구성되지 않았음을 의미할 수 있습니다.

문제가 해결될 때까지 다음 작업을 수행하세요.

- DataSync가 S3 버킷에 액세스할 수 있는지 확인합니다.
- DataSync 콘솔 또는 DescribeLocations3 작업을 사용하여 위치가 올바르게 구성되어 있는지 확인하세요.

오류: `FsS3HeadBucketFailed`

DataSync는 전송 중인 S3 버킷에 액세스할 수 없습니다. Amazon S3 HeadBucket 작업을 사용하여 DataSync에 버킷에 액세스할 권한이 있는지 확인하세요. 권한을 조정해야 하는 경우 DataSync에 S3 버킷 액세스 권한 제공 섹션을 참조하세요.

`Unable to list Azure Blobs on the volume root` 오류가 발생하여 작업 실패

DataSync 전송 작업이 `Unable to list Azure Blobs on the volume root`오류와 함께 실패하는 경우, 공유 액세스 서명(SAS) 토큰 또는 Azure스토리지 계정의 네트워크 관련 문제가 있을 수 있습니다.

취할 조치

다음을 시도하고 문제가 해결될 때까지 작업을 다시 실행하세요.

- SAS 토큰에 Microsoft Azure Blob Storage에 대한 액세스 권한이 있는지 확인하세요.
- 에서 DataSync 에이전트를 실행하는 경우, 에이전트가 상주하는 가상 네트워크에서 Azure의 액세스를 허용하도록 스토리지 계정을 구성하세요.
- Amazon EC2에서 에이전트를 실행하는 경우, 에이전트의 퍼블릭 IP 주소에서의 액세스를 허용하도록 Azure스토리지 방화벽을 구성하세요.

Azure 스토리지 계정의 네트워크를 구성하는 방법에 대한 자세한 설명은 Azure Blob Storage설명서를 참조하세요.

오류: `FsAzureBlobVolRootListBlobsFailed`

DataSync가 Microsoft Azure Blob Storage에 액세스하는 데 사용하는 공유 액세스 서명(SAS) 토큰에는 목록 권한이 없습니다.

문제를 해결하려면 목록 권한이 있는 토큰으로 위치를 업데이트하고 작업을 다시 실행해 보세요.

오류: `SrcLocHitAccess`

DataSync는 소스 위치에 액세스할 수 없습니다. DataSync에 해당 위치에 액세스할 수 있는 권한이 있는지 확인하고 작업을 다시 실행해 보세요.

오류: `SyncTaskErrorLocationNotAdded`

DataSync는 사용자의 위치에 액세스할 수 없습니다. DataSync에 해당 위치에 액세스할 수 있는 권한이 있는지 확인하고 작업을 다시 실행해 보세요.

오류: `S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation`

이 오류는 IAM 권한, Amazon S3 버킷 정책, AWS KMS 권한 또는 기타 권한 문제와 관련이 있을 수 있습니다. 이 오류가 발생하면 다음 정보를 사용하여 문제를 해결합니다.

- Amazon Simple Storage Service 사용 설명서의 Amazon S3의 액세스 거부(403 금지) 오류 문제 해결을 참조하세요.
- 에서 Amazon S3의 403 액세스 거부 오류를 해결하려면 어떻게 해야 합니까? AWS re:Post

`HeadObject` 또는 `GetObjectTagging` 오류와 함께 S3 소스 위치에서 작업 실패

`HeadObject` 또는 `GetObjectTagging` 관련 오류

S3 버킷에서 특정 버전 ID가 있는 객체를 전송하는 경우 HeadObject 또는 GetObjectTagging 관련 오류가 발생할 수 있습니다. 예를 들어 GetObjectTagging 관련 오류는 다음과 같습니다.

```
[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
```

이러한 오류 중 하나가 표시되면 DataSync가 S3 소스 위치에 액세스하는 데 사용하는 IAM 역할에 다음 권한이 있는지 확인합니다.

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

이러한 권한으로 역할을 업데이트해야 하는 경우 DataSync가 Amazon S3 위치에 액세스할 수 있도록 IAM 역할 생성 섹션을 참조하세요.

DataSync 작업 관련 문제 해결

다음 정보를 사용하여 AWS DataSync 작업 및 작업 실행 문제를 해결할 수 있습니다. 이러한 문제에는 작업 설정 문제, 중단된 작업 실행, 예상대로 전송되지 않은 데이터가 포함될 수 있습니다.

오류: 동기화 옵션 값이 잘못되었습니다. 옵션: TransferMode,PreserveDeletedFiles, 값: ALL,REMOVE

이 오류는 DataSync 작업을 만들거나 편집할 때 모든 데이터 전송 옵션을 선택하고 삭제된 파일 유지 옵션을 선택 취소할 때 발생합니다.

모든 데이터를 전송할 때 DataSync는 목적지 위치를 스캔하지 않으므로 무엇을 삭제해야 할지 모릅니다.

EniNotFound 오류와 함께 작업 실행 실패

이 오류는 Virtual Private Cloud(VPC)에서 작업의 네트워크 인터페이스 중 하나를 삭제하는 경우, 발생합니다. 작업이 예약되어 있거나 대기열에 있는 경우, 데이터 전송에 필요한 네트워크 인터페이스가 없으면 작업이 실패합니다.

취할 조치

이 문제를 해결할 수 있도록 다음 옵션이 제공됩니다:

- 작업을 수동으로 다시 시작합니다. 이렇게 하면 DataSync는 작업을 실행하는 데 필요한 누락된 네트워크 인터페이스를 생성합니다.
- VPC의 리소스를 정리해야 하는 경우, 아직 사용 중인 DataSync 작업과 관련된 네트워크 인터페이스를 삭제하지 마세요.

  작업에 할당된 네트워크 인터페이스를 보려면 다음 중 하나를 수행하세요:

  - DescribeTask 작업을 사용합니다. `SourceNetworkInterfaceArns` 및 `DestinationNetworkInterfaceArns`응답 요소에서 네트워크 인터페이스를 볼 수 있습니다.
  - Amazon EC2 콘솔에서 작업 ID(예: `task-f012345678abcdef0`)를 검색하여 해당 네트워크 인터페이스를 찾을 수 있습니다.
- 작업을 자동으로 실행하지 않는 것을 고려해 보세요. 여기에는 DataSync 또는 사용자 지정 자동화를 통해 작업 대기열 또는 스케줄링을 비활성화하는 것이 포함될 수 있습니다.

메모리를 할당할 수 없음 오류와 함께 작업 실행 실패

DataSync 작업이 실패하고 메모리를 할당할 수 없음 오류가 발생하면 몇 가지 다른 문제가 발생할 수 있습니다.

취할 조치

문제가 더 이상 나타나지 않을 때까지 다음을 시도해 보세요.

- 에이전트와 관련된 전송의 경우 에이전트가 가상 머신(VM) 또는 Amazon EC2 인스턴스 요구 사항을 충족하는지 확인합니다.
- 필터를 사용하여 전송을 여러 작업으로 나눕니다. 하나의 DataSync 작업이 처리할 수 있는 것보다 더 많은 파일이나 객체를 전송하려고 할 수 있습니다.

- 그래도 문제가 지속되면 지원으로 문의하세요.

FSx for ONTAP 파일 시스템에서 `Input/Output error`와 함께 작업 실패

FSx for ONTAP 파일 시스템을 사용하여 데이터를 전송할 때 DataSync 작업이 `Input/Output error`와 함께 실패하는 경우, 다음 중 하나 이상의 문제 때문일 수 있습니다.

FSx for ONTAP 볼륨의 최대 파일 용량 도달

이 오류는 볼륨에서 사용 가능한 inode 또는 파일 포인터 수가 소진되었을 때 발생합니다.

수행할 작업

먼저 볼륨의 최대 파일 용량을 확인합니다. 그 다음 inode 수나 스토리지 용량을 늘려 볼륨의 파일 용량을 늘립니다. 자세한 내용은 FSx for ONTAP 사용 설명서의 볼륨 파일 최대 용량 늘리기를 참조하세요.

FSx for ONTAP 볼륨의 사용 가능한 스토리지 용량 부족

이 오류는 볼륨에 사용 가능한 스토리지 용량이 없을 때 발생합니다.

수행할 작업

먼저, 볼륨의 사용 가능한 스토리지 용량을 확인합니다. 그 다음 볼륨의 스토리지 용량을 늘립니다. 자세한 내용은 FSx for ONTAP 사용 설명서의 볼륨 스토리지 용량 늘리기를 참조하세요.

> **Note**
>
> 필요한 경우 볼륨의 스토리지 용량을 자동으로 늘리려면 FSx for ONTAP 사용 설명서의 볼륨 자동 크기 조정 사용을 참조하세요.

FSx for ONTAP 디렉터리가 디렉터리별로 저장 가능한 최대 파일 수에 도달함

이 오류는 각 디렉터리에 저장할 수 있는 최대 파일 수에 도달했을 때 발생합니다.

취할 조치

더 큰 디렉터리를 지원하도록 최대 디렉터리 크기를 늘립니다. 자세한 내용은 AWS 권장 가이드의 FSx for ONTAP 최대 디렉터리 크기 사용 모범 사례를 참조하세요.

DataSync 작업 실행으로 인해 읽기 및 쓰기 동시성이 과도하게 발생하여 파일 시스템 처리량 용량을 높은 비율로 사용함

이 오류는 DataSync 작업 실행이 파일 시스템의 가용 처리량 용량을 너무 많이 사용하는 경우에 발생합니다.

수행할 작업

먼저 다음 방법을 사용하여 작업 실행이 파일 시스템의 처리량 용량을 너무 많이 사용하고 있는지 확인합니다.

- 사용 가능한 CloudWatch 지표를 사용하여 파일 시스템의 성능을 모니터링합니다. 자세한 내용은 FSx for ONTAP 사용 설명서의 파일 시스템 지표 모니터링을 참조하세요.
- Amazon FSx 콘솔에서 파일 시스템을 모니터링하여 파일 서버 성능 경고를 확인합니다. 자세한 내용은 FSx for ONTAP 사용 설명서의 성능 경고 및 권장 사항을 참조하세요.

그런 다음 작업이 파일 시스템의 가용 처리량 용량을 모두 사용하지 않도록 다음 중 하나를 수행합니다.

- 작업 실행의 대역폭 제한을 FSx for ONTAP 파일 시스템의 프로비저닝된 처리량 용량보다 낮은 값으로 설정합니다. 자세한 내용은 AWS DataSync 작업에 대한 대역폭 제한 설정 단원을 참조하십시오.
- 파일 시스템의 프로비저닝된 처리량 용량을 늘립니다. 자세한 내용은 FSx for ONTAP 사용 설명서의 처리량 용량 업데이트를 참조하세요.

FSx for ONTAP 파일 시스템에 대한 `Connection Reset by peer` 또는 `Host is down` 메시지와 함께 작업 실패

FSx for ONTAP 파일 시스템을 사용하여 데이터를 전송할 때 DataSync 작업이 `Connection Reset by peer` 또는 `Host is down` 메시지와 함께 실패하는 경우, 다음 중 하나 이상의 문제 때문일 수 있습니다.

- 작업 실행 중 파일 시스템의 SMB 서버가 재부팅되었거나 연결이 끊어졌습니다.
- 작업 실행 중 파일 시스템이 기본 서버에서 보조 서버(및 IP 주소)로 장애 조치되었습니다. DataSync는 작업 실행 중에 보조 IP 주소로 장애 조치를 지원하지 않습니다.

  FSx for ONTAP 파일 시스템은 다음 이벤트 중에 보조 서버 및 IP 주소로 장애 조치됩니다.

  - 기본 서버를 사용할 수 없게 됨.

- 기본 서버의 가용 영역을 사용할 수 없게 됨(다중 AZ 파일 시스템의 경우).
- 사용자가 시작한 처리량 용량 변경 작업 동안.
- 파일 시스템의 정기 예약된 유지 관리 기간 동안.

자세한 내용은 FSx for ONTAP 사용 설명서의 FSx for ONTAP 장애 조치 프로세스를 참조하세요.

취할 조치

작업을 다시 시작합니다.

작업 실행이 시작 상태이지만 아무 일도 일어나지 않음

일반적으로 에이전트의 전원이 꺼져 있거나 네트워크 연결이 끊겼기 때문에 DataSync 작업이 시작하는 중 상태에서 멈출 수 있습니다.

취할 조치

에이전트의 상태가 온라인인지 확인하세요. 에이전트가 오프라인 상태인 경우, 전원이 켜져 있는지 확인하세요.

에이전트의 전원을 켰는데 작업이 여전히 출범하는 중 상태라면 에이전트와 AWS사이의 네트워크 연결 문제가 발생했을 가능성이 무엇보다도 높습니다. 네트워크 연결을 테스트하는 방법에 대한 정보는 에이전트의 DataSync 서비스 연결 확인섹션을 참조하세요.

이 문제가 계속되면 상담원에게 무슨 일이 벌어지고 있는지 모르겠어요. 누군가 저를 도와줄 수 있나요?단원을 참조하세요.

작업 실행이 준비 상태에서 중단됨

DataSync 전송 작업이 준비 상태에 머무르는 시간은 전송 소스 및 대상의 데이터 양과 해당 스토리지 시스템 성능에 따라 달라집니다.

작업이 시작되면 DataSync는 재귀적 디렉터리 리스팅 작업을 수행하여 소스와 목적지의 모든 파일, 객체, 디렉터리, 메타데이터를 검색합니다. DataSync는 이러한 목록을 사용하여 스토리지 시스템 간의 차이점을 식별하고 복제할 대상을 결정합니다. 이 프로세스는 몇 분 또는 몇 시간이 걸릴 수 있습니다.

취할 조치

아무 조치도 취하지 않아도 됩니다. 작업 상태가 전송 중으로 변경될 때까지 계속 기다리세요. 상태가 여전히 변경되지 않으면 AWS Support 센터로 문의하세요.

전송 완료 전 작업 실행이 중지됨

DataSync 작업 실행이 조기에 중지되면 작업 구성에 AWS 계정에서 비활성화된 AWS 리전 이 포함될 수 있습니다.

취할 조치

작업을 다시 실행하려면 다음을 수행합니다.

1. 작업 리전의 옵트인 상태를 확인하고 활성화되어 있는지 확인합니다.
2. 작업을 다시 시작합니다.

Google Cloud Storage 버킷에서 전송 시 작업 실행 실패

DataSync는 Amazon S3 API를 사용하여 Google 클라우드 스토리지와 통신하기 때문에 객체 태그를 복사하려고 하면 DataSync 전송의 실패를 야기할 수 있는 제한이 있습니다. 이 문제와 관련된 다음 메시지가 CloudWatch 로그에 나타납니다.

[경고] /*your-bucket*/*your-object* 파일에 대한 메타데이터를 읽지 못함: S3 객체 태깅 가져오기 실패: 태그를 지정하지 않고 진행

이를 방지하려면 전송 작업 설정을 구성할 때 객체 태그 복사 옵션을 선택 취소하세요.

작업 실행 타임스탬프 간 불일치

DataSync 콘솔 또는 Amazon CloudWatch Logs를 확인할 때 DataSync 작업 실행의 시작 및 종료 시간이 다른 모니터링 도구에 표시되는 타임스탬프와 일치하지 않음을 확인할 수 있습니다. 이는 콘솔과 CloudWatch Logs가 작업 실행이 시작 또는 대기 상태에 머무른 시간을 포함하는 반면, 일부 다른 도구에서는 이를 포함하지 않기 때문입니다.

DataSync 콘솔 또는 CloudWatch Logs의 실행 타임스탬프를 다음 위치들과 비교하는 경우 이러한 불일치를 확인할 수 있습니다.

- 전송과 관련된 파일 시스템의 로그
- DataSync가 데이터를 쓴 Amazon S3 객체의 마지막 수정 날짜
- DataSync 에이전트에서 들어오는 네트워크 트래픽
- Amazon EventBridge 이벤트

`NoMem` 오류가 발생하여 작업 실행 실패

전송하려는 데이터 세트가 DataSync에 비해 너무 클 수 있습니다. 이 오류가 표시되면 AWS Support 센터에 문의하세요.

`FsNfsIdMappingEnabled` 오류가 발생하여 작업 실행 실패

DataSync는 NFSv4 ID 매핑을 지원하지 않습니다. 이 문제를 해결하려면 NFSv3를 사용하도록 NFS 위치를 구성합니다.

객체가 `user metadata key` 오류로 Azure Blob Storage로 전송되지 않음

S3 버킷에서 Azure Blob Storage로 전송할 때 다음 오류가 표시될수 있습니다.

```
[ERROR] Failed to transfer file /user-metadata/file1: Azure Blob user metadata key must
 be a CSharp identifier
```

즉, */user-metadata/file1*에는 유효한 C# 식별자를 사용하지 않는 사용자 메타데이터가 포함됩니다. 자세한 설명은 Microsoft 설명서를 참조하세요.

대상 위치에 `/.aws-datasync` 폴더가 있음

DataSync는 대상 위치에 `/.aws-datasync`라는 폴더를 생성하여 데이터 전송을 용이하게 합니다.

DataSync는 일반적으로 전송 후 이 폴더를 삭제하지만, 그렇지 않은 상황이 발생할 수 있습니다.

취할 조치

실행 중인 작업 실행이 해당 위치에 복사되지 않는 한 언제든지 이 폴더를 삭제합니다.

SMB를 사용하여 위치 간에 심볼 링크를 전송할 수 없음

작업 실행이 완료되면 다음 오류가 표시됩니다.

```
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.
```

SMB 스토리지 시스템(예: SMB 파일 서버 및 Amazon FSx for Windows File Server 파일 시스템) 간 전송 시 CloudWatch 로그에 다음과 같은 경고 및 오류가 표시될 수 있습니다.

```
[WARN] Failed to read metadata for file /appraiser/symlink: No data available
```

```
[ERROR] Failed to read metadata for directory /appraiser/symlink: No data available
```

취할 조치

이러한 위치 유형 간에 전송하는 경우 DataSync는 심볼 링크(또는 하드 링크) 전송을 지원하지 않습니다. 자세한 내용은 에서 복사한 링크 및 디렉터리 AWS DataSync 단원을 참조하십시오.

작업 보고서 오류

작업 보고서로 DataSync 전송을 모니터링하려고 할 때 다음 오류 중 하나가 발생할 수 있습니다.

오류 메시지	차선책
파일 경로가 최대 길이인 4,096자를 초과합니다. 작업 보고서에 쓸 수 없습니다.	없음. DataSync는 경로가 4,096바이트를 초과하는 파일을 전송할 수 없습니다. 자세한 내용은 스토리지 시스템, 파일, 객체 제한 단원을 참조하십시오.
잘못된 버킷 또는 IAM 역할로 인해 작업 보고서를 S3에 업로드할 수 없습니다.	DataSync IAM 역할에 작업 보고서를 S3 버킷에 업로드할 수 있는 적절한 권한이 있는지 확인하세요.
태스크 보고서를 생성하기 전에 실행 오류가 발생했습니다.	CloudWatch 로그를 확인하여 작업 실행이 실패한 이유를 확인하세요.

데이터 확인 문제 해결

기본적으로 AWS DataSync 는 전송이 끝날 때 데이터의 무결성을 확인합니다. 다음 정보를 사용하면 DataSync가 데이터 확인을 완료하기 전에 수정 또는 삭제되는 파일 등의 일반적인 확인 오류 및 경고를 진단하는 데 도움이 됩니다.

확인 문제가 발생하면 표시되는 작업 실행 오류 외에도 CloudWatch Logs(또는 작업 보고서)를 함께 검토하는 것이 종종 도움이 됩니다. DataSync는 확장 모드 작업에는 JSON 정형 로그를 제공하고, 기본 모드 작업에는 비정형 로그를 제공합니다.

파일 콘텐츠 간에 불일치가 있습니다.

작업 실행이 완료되면 다음 오류가 표시됩니다.

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

CloudWatch Logs에서 소스 위치와 대상 위치 간에 콘텐츠가 달라 확인에 실패할 수 있습니다. 전송 중에 파일이 수정되는 경우 이 문제가 발생할 수 있습니다.

예를 들어 다음 로그는 mtime, srcHash, dstHash 값이 서로 다른 file1.txt를 보여줍니다.

기본 모드 로그 예시

```
[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
```

DataSync에서 mtime은 준비 전에 파일을 마지막으로 쓴 시간을 나타냅니다. 전송을 확인할 때 DataSync는 소스 위치와 대상 위치 간의 mtime 값을 비교합니다. 파일의 mtime이 두 위치에서 동일하지 않은 경우 이와 같은 확인 실패가 발생합니다. srcHash와 dstHash가 다르다는 것은 두 위치에서 파일의 내용이 일치하지 않음을 나타냅니다.

취할 조치

해결 방법:

1. 에포크 시간 변환기를 사용하여 소스 파일, 대상 파일, 객체 중 더 최근에 수정된 항목을 확인합니다. 이는 최신 버전을 식별하는 데 도움이 될 수 있습니다.
2. 이 오류가 다시 발생하지 않도록 소스 및 대상에 활동이 없는 유지 관리 기간 동안 작업을 실행하도록 예약합니다.

파일의 SMB 메타데이터 간에 불일치가 있습니다.

작업 실행이 완료되면 다음 오류가 표시됩니다.

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

SMB(Server Message Block) 프로토콜을 지원하는 스토리지 시스템 간 전송 시, 파일의 확장 SMB 속성이 소스와 대상 간에 일치하지 않는 경우 이 오류가 표시될 수 있습니다.

예를 들어 다음 로그는 `file1.txt`가 위치 간에 다른 `extAttrsHash` 값을 가지고 있음을 보여줍니다. 이는 파일 내용이 동일하지만 확장 속성이 대상에 설정되지 않았음을 나타냅니다.

기본 모드 로그 예시

```
[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
```

확장 속성에 대한 관련 오류 메시지가 표시될 수도 있습니다.

```
[ERROR] Deferred error: WriteFileExtAttr2 failed to setextattrlist(filename="/
directory1/directory2/file1.txt"): Input/output error
```

취할 조치

이 오류는 일반적으로 액세스 제어 목록(ACL)을 대상으로 복사할 권한이 충분하지 않을 때 발생합니다. 이 문제를 해결하려면 대상 유형에 따라 다음 구성 가이드를 검토하세요.

- FSx for Windows File Server 파일 시스템의 필수 권한
- SMB를 사용하는 FSx for ONTAP 파일 시스템의 필수 권한

전송할 파일이 현재 소스 위치에 없음

작업 실행이 완료되면 다음 오류가 표시됩니다.

```
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.
```

파일이 소스 위치에 없음을 나타내는 오류가 로그에 표시될 수 있습니다. 이는 준비 후 DataSync가 파일을 전송하기 전에 해당 파일(예: `file1.dll` 및 `file2.dll`)을 삭제하는 경우 발생할 수 있습니다.

기본 모드 로그 예시

```
[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
```

취할 조치

이러한 상황을 방지하려면 소스 위치에 활동이 없을 때 작업을 실행하도록 예약합니다.

예를 들어 사용자와 애플리케이션이 해당 위치에서 활발히 작업하지 않는 유지 관리 기간 동안 해당 작업을 실행할 수 있습니다.

경우에 따라 이 오류와 관련된 로그가 표시되지 않을 수 있습니다. 이 경우 AWS Support 센터에 문의하세요.

DataSync가 대상 데이터를 확인할 수 없음

작업 실행이 완료되면 다음 오류가 표시됩니다.

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

로그에서, DataSync가 대상 위치의 특정 폴더 또는 파일을 확인하지 못했음을 확인할 수 있습니다. 이러한 오류는 다음과 같습니다.

기본 모드 로그 예시

```
[ERROR] Failed to read metadata for destination file /directory1/directory2/
file1.txt: No such file or directory
```

파일의 경우 다음과 같은 확인 실패가 표시될 수 있습니다.

기본 모드 로그 예시

```
[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
```

취할 조치

이러한 로그는 전송 후 대상 데이터를 확인하기 전에 대상 데이터가 삭제되었음을 나타냅니다. (로그는 데이터가 같은 기간에 소스 위치로 업로드될 때도 비슷하게 나타남)

이러한 상황을 방지하려면 대상 위치에 활동이 없을 때 작업을 실행하도록 예약합니다.

예를 들어 사용자와 애플리케이션이 해당 위치에서 활발히 작업하지 않는 유지 관리 기간 동안 해당 작업을 실행할 수 있습니다.

DataSync가 객체 메타데이터를 읽을 수 없음

작업 실행이 완료되면 다음 오류가 표시됩니다.

```
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.
```

로그에서, 실패한 Amazon S3 `HeadObject` 요청으로 인해 DataSync가 `file1.png`를 읽지 못했음을 확인할 수 있습니다. DataSync는 작업 준비 및 확인 중에 S3 위치에 대해 `HeadObject` 요청을 수행 합니다.

기본 모드 로그 예시

```
[WARN] Failed to read metadata for file /file1.png: S3 Head Object Failed
```

취할 조치

이 문제를 해결하려면 DataSync에 S3 버킷을 사용할 적절한 수준의 권한이 있는지 확인합니다.

- DataSync가 Amazon S3 위치에 액세스하는 데 사용하는 IAM 역할이 `s3:GetObject` 권한을 허용하는지 확인합니다. 자세한 내용은 필수 권한 단원을 참조하십시오.
- S3 버킷이 서버 측 암호화를 사용하는 경우 DataSync가 해당 버킷의 객체에 액세스할 수 있는지 확인합니다. 자세한 내용은 서버측 암호화를 사용하여 S3 버킷에 액세스 단원을 참조하십시오.

객체의 시스템 정의 메타데이터 불일치

S3 버킷 간 확장 모드 작업 실행이 완료되면 다음 오류가 표시됩니다.

```
Verification failed due to a difference in metadata
```

로그에서 객체의 Amazon S3 시스템 정의 메타데이터가 일치하지 않음을 확인할 수 있습니다. 이 특정 예시에서는 소스 객체에 `Content-Type` 메타데이터가 없지만 대상 객체에는 메타데이터가 있습니다. 이는 DataSync가 객체를 전송할 때 대상 S3 버킷이 객체에 `"ContentType": "application/octet-stream"` 메타데이터를 자동으로 적용했기 때문입니다.

확장 모드 로그 예시


```
{
    "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"
}
```

취할 조치

이 오류를 방지하려면 Content-Type 메타데이터 속성을 포함하도록 소스 위치 객체를 업데이트합니다.

데이터 확인 기간 이해

DataSync 확인에는 파일 내용에 대한 SHA256 체크섬과 위치 간 파일 메타데이터에 대한 정확한 비교가 포함됩니다. 확인에 걸리는 시간은 관련된 파일 또는 객체 수, 스토리지 시스템의 데이터 크기, 이러한 시스템의 성능 등 여러 요인에 따라 달라집니다.

취할 조치

확인 시간에는 여러 요인이 영향을 미치므로, 별도로 조치할 필요는 없습니다. 그러나 작업 실행이 확인 중 상태에서 멈춘 것 같다면 AWS Support 센터에 문의하세요.

DataSync를 사용한 예상보다 높은 S3 스토리지 비용 문제 해결

AWS DataSync 전송 후 Amazon S3 스토리지 비용이 생각보다 높다면 다음 이유 중 하나 이상이 원인일 수 있습니다.

- S3 버킷으로 또는 S3 버킷에서 전송할 때 DataSync에서 수행한 S3 API 요청과 관련된 비용이 발생합니다.
- DataSync는 Amazon S3 다파트 업로드 기능을 사용하여 객체를 S3 버킷에 업로드합니다. 그 결과, 제대로 완료되지 않은 업로드에 예기치 않은 스토리지 요금이 부과될 수 있습니다.
- DataSync는 콘솔에서 객체 태그 복사가 활성화되거나 `ObjectTags`가 `PRESERVE`으로 설정된 경우 소스 및 대상 객체에서 객체 태그를 복사합니다. 이러한 객체 태그를 복사하면 S3 API 요청 비용이 발생할 수 있습니다.
- S3 버킷에서 객체 버전 관리가 활성화된 상태일 수 있습니다. 객체 버전 관리가 활성화되면 Amazon S3는 명칭이 동일한 객체의 여러 사본을 저장합니다.

취할 조치

이 경우에는 다음 단계를 수행할 수 있습니다.

- DataSync에서 S3 요청을 사용하는 방식과 이러한 요청이 스토리지 비용에 어떤 영향을 미칠 수 있는지 이해해야 합니다. 자세한 내용은 DataSync 사용 시 S3 요청 비용 평가 단원을 참조하십시오.
- 문제가 멀티파트 업로드와 관련된 경우 미완료 멀티파트 업로드 항목을 정리하도록 S3 버킷의 멀티파트 업로드 정책을 구성하여 스토리지 비용을 줄이세요. 자세한 내용은 AWS 블로그 게시물 S3 수명 주기 관리 업데이트 - 멀티파트 업로드 및 마커 삭제 지원을 참조하세요.
- 객체 태그 복사와 관련된 문제로 객체 태그가 필요하지 않은 경우 DataSync 콘솔에서 객체 태그 복사 확인란의 선택을 취소하거나 작업 생성, 시작, 업데이트 시 `ObjectTags`를 `None`으로 설정합니다.
- 객체 버전 관리와 관련된 문제인 경우, S3 버킷의 객체 버전 관리를 비활성화하세요.

추가 도움이 필요한 경우 AWS Support 센터에 문의하세요.

AWS DataSync 자습서

이 자습서에서는 AWS DataSync을 사용하여 몇 가지 실제 시나리오를 안내합니다.

주제

- 자습서:를 통해 온프레미스 스토리지에서 Amazon S3로 데이터 전송 AWS 계정
- 자습서:에서 Amazon S3 버킷 간에 데이터 전송 AWS 계정

자습서:를 통해 온프레미스 스토리지에서 Amazon S3로 데이터 전송 AWS 계정

온프레미스 스토리지 AWS DataSync 와 함께를 AWS 사용하는 경우 일반적으로 DataSync 에이전트 AWS 계정 와 동일한에 속하는 스토리지 서비스로 데이터를 전송합니다. 하지만 다른 계정과 연계된 Amazon S3 버킷으로 데이터를 전송해야 하는 경우도 있습니다.

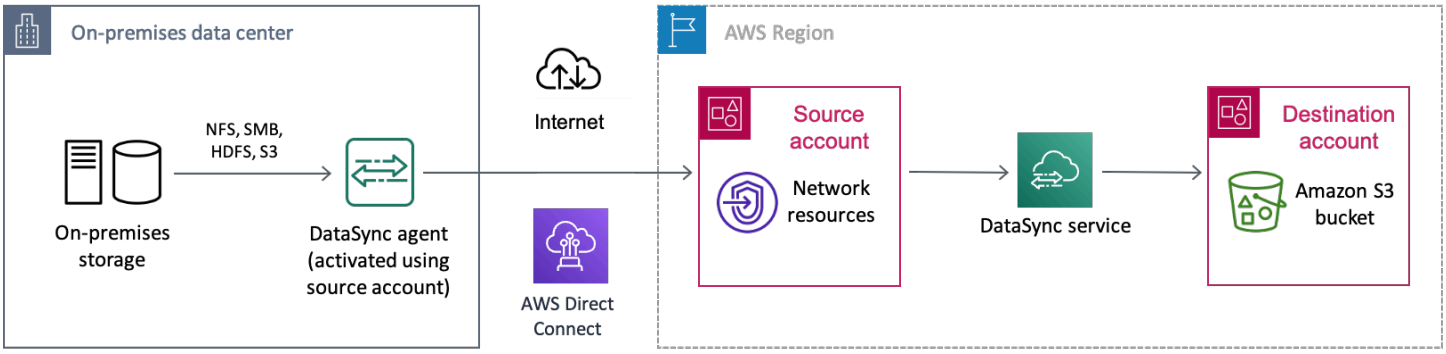
> **Important**
>
> 이 자습서의 메서드를 AWS 계정 사용하여 간에 데이터를 전송하는 것은 Amazon S3가 DataSync 전송 위치 중 하나인 경우에만 작동합니다.

개요

AWS 계정특히 조직의 리소스를 관리하는 별도의 팀이 있는 경우 서로 다른 간에 데이터를 전송해야 하는 경우는 드물지 않습니다. DataSync를 사용한 계정간 전송은 다음과 같습니다:

- 소스 계정: 네트워크 리소스를 관리하기 AWS 계정 위한 입니다. DataSync 에이전트를 활성화하는 데 사용할 계정입니다.
- 대상 계정: 데이터를 전송해야 하는 S3 버킷을 관리하기 AWS 계정 위한 입니다.

다음 다이어그램은 이 종류의 시나리오를 나타냅니다



사전 조건: 필수 소스 계정 권한

소스의 경우 이러한 종류의 교차 계정 전송과 함께 고려해야 할 두 가지 권한 세트 AWS 계정가 있습니다.

- 사용자가 DataSync를 사용하도록 허용하는 사용자 권한(사용자 또는 스토리지 관리자일 수 있음)입니다. 이러한 권한을 통해 DataSync 위치 및 작업을 생성할 수 있습니다.
- DataSync가 대상 계정 버킷으로 데이터를 전송하도록 허용하는 DataSync 서비스 권한입니다.

User permissions

소스 계정에서 DataSync 위치 및 작업을 생성하기 위해 IAM 역할에 최소한 다음 권한을 추가합니다. 역할에 권한을 추가하는 방법에 대한 자세한 내용은 IAM 역할 생성 또는 수정을 참조하세요.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "SourceUserRolePermissions",
            "Effect": "Allow",
            "Action": [
                "datasync:CreateLocationS3",
                "datasync:CreateTask",
                "datasync:DescribeLocation*",
                "datasync:DescribeTaskExecution",
                "datasync:ListLocations",
                "datasync:ListTaskExecutions",
                "datasync:DescribeTask",
                "datasync:CancelTaskExecution",
                "datasync:ListTasks",
                "datasync:StartTaskExecution",
```

```
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:ListRoles",
                "iam:CreatePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DataSync-*"
        },
        {
            "Sid": "IAMAttachRolePermissions",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DataSync-*",
            "Condition": {
            "ArnLike": {
                "iam:PolicyARN": [
                   "arn:aws:iam::111122223333:policy/DataSync-*",
                   "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
                   "arn:aws:iam::aws:policy/service-role/AWSDataSyncFullAccess"
                ]
            }
          }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
```

```
            }
        }
    ]
}
```

> **Tip**
>
> 사용자 권한을 설정하려면 AWSDataSyncFullAccess 사용을 고려하세요. 이는 사용자에게 DataSync에 대한 전체 액세스 권한과 해당 종속성에 대한 최소 액세스를 제공하는 AWS 관리형 정책입니다.

DataSync service permissions

대상 계정 버킷으로 데이터를 전송하려면 DataSync 서비스는 소스 계정에서 다음 권한이 필요합니다.

이 자습서의 후반부에서 DataSync에 대한 IAM 역할을 생성할 때 이러한 권한을 추가합니다. 또한 대상 버킷 정책 및 DataSync 대상 위치 생성 시 이 역할(*source-datasync-role*)을 지정합니다.

```
{
  "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/*"
    }
  ]
}
```

사전 조건: 필수 대상 계정 권한

대상 계정에서 사용자 권한을 통해 대상 버킷의 정책을 업데이트하고 해당 액세스 제어 목록(ACL)을 비활성화할 수 있어야 합니다. 이러한 특정 권한에 대한 자세한 설명은 Amazon S3 사용자 가이드https://docs.aws.amazon.com/AmazonS3/latest/userguide/를 참조하세요.

1단계: 소스 계정에서 DataSync 에이전트를 생성합니다.

시작하려면 온프레미스 스토리지 시스템에서 읽고 DataSync 서비스와 통신할 수 있는 DataSync 에이전트를 생성해야 합니다. 이 프로세스에는 온프레미스 스토리지 환경에 에이전트를 배포하고 소스 AWS 계정에서 에이전트를 활성화하는 작업이 포함됩니다.

> **Note**
>
> 이 자습서의 단계는 사용하는 모든 타입의 에이전트 및 서비스 엔드포인트에 적용됩니다.

DataSync 에이전트를 만들려면

1. 온프레미스 스토리지 환경에 DataSync 에이전트를 배포합니다.
2. 에이전트가 통신하는 데 사용할 서비스 엔드포인트를 선택합니다 AWS.
3. 소스 계정에서 에이전트를 활성화하세요.

2단계: 소스 계정에서 대상 버킷 액세스의 DataSync IAM 역할 생성

소스 계정에는 DataSync가 대상 계정 버킷에 데이터를 전송할 권한을 부여하는 IAM 역할이 필요합니다.

계정 간에 데이터를 이전하는 것이므로 이 역할을 수동으로 생성해야 합니다. (DataSync는 동일한 계정으로 전송할 때 콘솔에서 이 역할을 생성할 수 있습니다.)

DataSync IAM 역할 생성

DataSync를 신뢰할 수 있는 엔터티로 사용하여 IAM 역할을 생성합니다.

IAM 역할을 만들려면

1. 소스 계정으로 AWS Management Console 에 로그인합니다.
2. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
3. 왼쪽 탐색 창의 액세스 관리에서 역할을 선택한 다음, 역할 생성을 선택합니다.
4. 신뢰할 수 있는 엔터티 선택 페이지에서 신뢰할 수 있는 엔터티 유형으로 AWS 서비스를 선택합니다.
5. 사용 사례로 드롭다운 목록에서 DataSync를 선택하고 DataSync를 선택합니다. 다음을 선택합니다.
6. 권한 추가 페이지에서 다음을 선택합니다.
7. 역할 이름을 제공하고 역할 생성을 선택합니다.

자세한 내용은 IAM 사용 설명서의 AWS 서비스 (콘솔)에 대한 역할 생성을 참조하세요.

DataSync IAM 역할에 권한 추가

방금 생성한 IAM 역할에는 DataSync가 대상 계정의 S3 버킷에 데이터를 전송하도록 허용하는 권한이 필요합니다.

IAM 역할에 권한을 추가하려면

1. IAM 콘솔의 역할 페이지에서 방금 생성한 역할을 찾아서 그 명칭을 선택합니다.
2. 역할의 세부 정보 페이지에서 권한 탭을 선택합니다. 권한 추가를 선택한 후 인라인 정책 추가를 선택합니다.
3. JSON 탭을 선택한 다음, 다음을 수행합니다.

   a. 다음 JSON을 정책 편집기에 붙여넣습니다.

> **Note**
>
> `aws:ResourceAccount`의 값은 정책에 명시된 Amazon S3 버킷을 소유한 계정의 ID여야 합니다.

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. *amzn-s3-demo-destination-bucket*의 각 인스턴스를 대상 계정의 S3 버킷의 이름으로 바꿉니다.

4. 다음을 선택합니다. 정책 명칭을 지정하고 정책 생성을 선택합니다.

3단계: 대상 계정에서 S3 버킷 정책 업데이트

대상 계정에서, 소스 계정에서 생성한 DataSync IAM 역할을 포함하도록 대상 S3 버킷 정책을 수정합니다.

시작하기 전에: 대상 계정에 필요한 권한이 있는지 확인합니다.

목적지 S3 버킷 정책을 업데이트하려면

1. 에서 대상 계정으로 AWS Management Console전환합니다.
2. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
3. 왼쪽 탐색 창에서 버킷을 선택합니다.
4. 버킷 목록에서 데이터를 전송할 S3 버킷을 선택합니다.
5. 버킷의 세부 정보 페이지에서 권한 탭을 선택합니다.
6. 버킷 정책에서 편집을 선택하고 다음을 수행하여 S3 버킷 정책을 수정하세요.

   a. 편집기에 있는 내용을 업데이트하여 다음 정책 설명을 포함하세요.

      JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/source-datasync-role"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
```

```
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

b. *source-account*의 각 인스턴스를 소스 계정의 AWS 계정 ID로 바꾸세요.

c. *source-datasync-role*을 소스 계정에서 DataSync용으로 생성한 IAM 역할로 바꾸세요.

d. *amzn-s3-demo-destination-bucket*의 각 인스턴스를 대상 계정의 S3 버킷의 이름으로 바꿉니다.

7. 변경 사항 저장을 선택합니다.

4단계: 목적지 계정에서 S3 버킷의 ACL을 비활성화합니다.

S3 버킷에 복사하는 모든 데이터는 귀하의 목적지 계정에 속한다는 사실이 중요합니다. 이 계정이 데이터를 소유하도록 하려면 버킷의 액세스 제어 목록(ACL)을 비활성화하십시오. 자세한 설명은 Amazon S3 사용자 가이드의 객체 소유권 제어 및 버킷에 대해 ACL 사용 중지를 참조하세요.

대상 버킷에 대한 ACL을 비활성화하려면

1. 대상 계정으로 S3 콘솔에 로그인한 상태에서 데이터를 전송할 S3 버킷을 선택합니다.
2. 버킷의 세부 정보 페이지에서 권한 탭을 선택합니다.
3. 객체 소유권(Object Ownership)에서 편집(Edit)을 선택합니다.
4. 아직 선택하지 않은 경우, ACL 비활성화(권장) 옵션을 선택하세요.
5. 변경 사항 저장을 선택합니다.

5단계: 소스 계정에서 온프레미스 스토리지를 위한 DataSync 소스 위치 생성

소스 계정에서 데이터를 전송하는 온프레미스 스토리지 시스템의 DataSync 소스 위치를 생성합니다. 이 위치에서는 소스 계정에서 활성화한 에이전트를 사용합니다.

6단계: 소스 계정에서 S3 버킷의 DataSync 목적지 위치를 생성합니다.

소스 계정에 있는 동안 데이터를 전송하려는 S3 버킷의 위치를 생성합니다.

시작하기 전에: 소스 계정에 필요한 권한이 있는지 확인합니다.

DataSync 콘솔 인터페이스를 사용하여 교차 계정 위치를 생성할 수 없으므로 이 지침에 따라 대상 위치를 생성하는 `create-location-s3` 명령을 실행해야 합니다. 콘솔에서 직접 시작하는 브라우저 기반 사전 인증된 AWS CloudShell쉘을 사용하여 명령을 실행하는 것이 좋습니다. CloudShell을 사용하면 AWS CLI 명령줄 도구를 다운로드하거나 설치`create-location-s3`하지 않고도와 같은 명령을 실행할 수 있습니다.

> **Note**
>
> CloudShell 이외의 명령줄 도구를 사용하여 다음 단계를 완료하려면 AWS CLI 프로필이 소스 계정에서 DataSync를 사용하는 데 필요한 사용자 권한을 포함하는 동일한 IAM 역할을 사용하는지 확인하세요.

CloudShell을 사용하여 DataSync 목적지 위치를 만들려면

1. 소스 계정에 있는 동안 다음 중 하나를 수행하여 콘솔에서 CloudShell을 시작합니다.
   - 콘솔 탐색 모음에서 CloudShell 아이콘을 선택합니다. 검색 상자 오른쪽에 있습니다.
   - 콘솔 탐색 모음의 검색 상자를 사용하여 CloudShell을 검색한 다음 CloudShell 옵션을 선택합니다.
2. 다음 명령을 복사합니다.

```
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. 대상 계정에서 *amzn-s3-demo-destination-bucket*을 S3 버킷의 이름으로 바꿉니다.
4. *source-user-account*을 소스 계정의 AWS 계정 ID로 바꾸십시오.
5. *source-datasync-role*을 소스 계정에서 생성한 DataSync IAM 역할로 대체하세요.
6. 명령을 CloudShell에서 실행합니다.

   명령이 다음과 비슷한 DataSync 위치 ARN을 반환하면 위치가 성공적으로 생성된 것입니다.

   ```
   {
     "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
   abcdef01234567890"
   }
   ```

7. 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 위치를 선택합니다.

소스 계정에서 대상 계정 버킷용으로 방금 생성한 S3 위치를 확인할 수 있습니다.

7단계: 소스 계정에서 DataSync 전송 작업을 생성하고 시작

DataSync 작업을 시작하여 데이터를 전송하기 전에 지금까지 수행한 작업을 요약해 보겠습니다.

- 소스 계정에서 DataSync 에이전트를 생성했습니다. 에이전트는 온프레미스 스토리지 시스템에서 읽고 DataSync 서비스와 통신할 수 있습니다.
- 소스 계정에서 DataSync가 대상 계정의 S3 버킷에 데이터를 전송하도록 허용하는 IAM 역할을 생성했습니다.
- 대상 계정에서 DataSync가 S3 버킷으로 데이터를 전송할 수 있도록 S3 버킷을 구성했습니다.
- 소스 계정에서 전송을 위한 DataSync 소스 및 목적지 위치를 생성했습니다.

DataSync 작업을 생성하고 시작하려면

1. 소스 계정에서 DataSync 콘솔을 계속 사용하는 동안 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 작업과 작업 생성을 선택합니다.
2. 소스 위치 구성 페이지에서 기존 위치 선택을 선택합니다. 온프레미스 스토리지의 데이터를 복사할 소스 위치를 선택한 후 다음을 선택합니다.
3. 목적지 위치 구성 페이지에서 기존 위치 선택을 선택합니다. 데이터를 복사할 목적지 위치(목적지 계정의 S3 버킷) 를 선택하고 다음을 선택합니다.
4. 설정 구성 페이지에서 작업 이름을 지정합니다. 필요에 따라 Amazon CloudWatch 로그 그룹 지정과 같은 추가 설정을 구성합니다. 다음을 선택합니다.

5. 검토 페이지에서 설정을 검토하고 작업 생성을 선택합니다.
6. 작업의 세부 정보 페이지에서 시작을 선택하고 다음 중 하나를 선택하세요:
   - 수정하지 않고 작업을 실행하려면 기본값으로 시작을 선택합니다.
   - 작업을 실행하기 전에 수정하려면 재정의 옵션으로 시작을 선택합니다.

작업이 완료되면 목적지 계정의 S3 버킷을 확인합니다. 소스 위치에서 이동한 데이터를 확인할 수 있어야 합니다.

관련 리소스

이 자습서에서 수행한 것에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 에 대한 역할 생성 AWS 서비스 (콘솔)
- 역할 신뢰 정책 수정(콘솔)
- Amazon S3 콘솔을 사용하여 버킷 정책 추가
- 를 사용하여 S3 위치 생성 AWS CLI

자습서:에서 Amazon S3 버킷 간에 데이터 전송 AWS 계정

를 사용하면 다른에 속하는 Amazon S3 버킷 간에 데이터를 전송할 AWS DataSync수 있습니다 AWS 계정.

> **Important**
>
> 이 자습서의 메서드를 AWS 계정 사용하여 간에 데이터를 전송하는 작업은 Amazon S3에서만 가능합니다. 또한 이 자습서는 서로 다른 AWS 리전의 S3 버킷 간에 데이터를 전송하는 데 도움이 될 수 있습니다.

개요

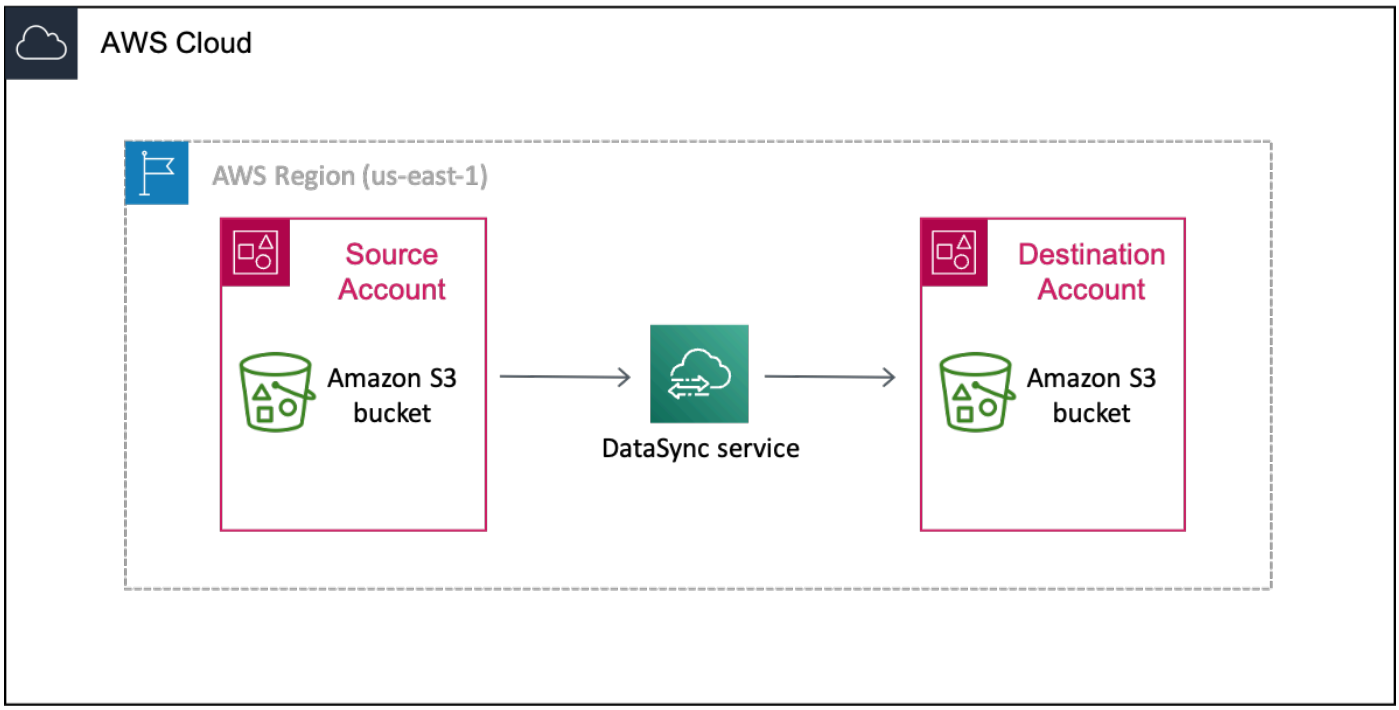
AWS 계정특히 조직의 리소스를 관리하는 별도의 팀이 있는 경우 간에 데이터를 전송하는 것은 드문 일이 아닙니다. DataSync를 사용한 계정간 전송은 다음과 같습니다:

- 소스 계정: 데이터를 전송해야 하는 S3 버킷을 관리하기 AWS 계정 위한 입니다.

- 대상 계정: 데이터를 전송해야 하는 S3 버킷을 관리하기 AWS 계정 위한 입니다.

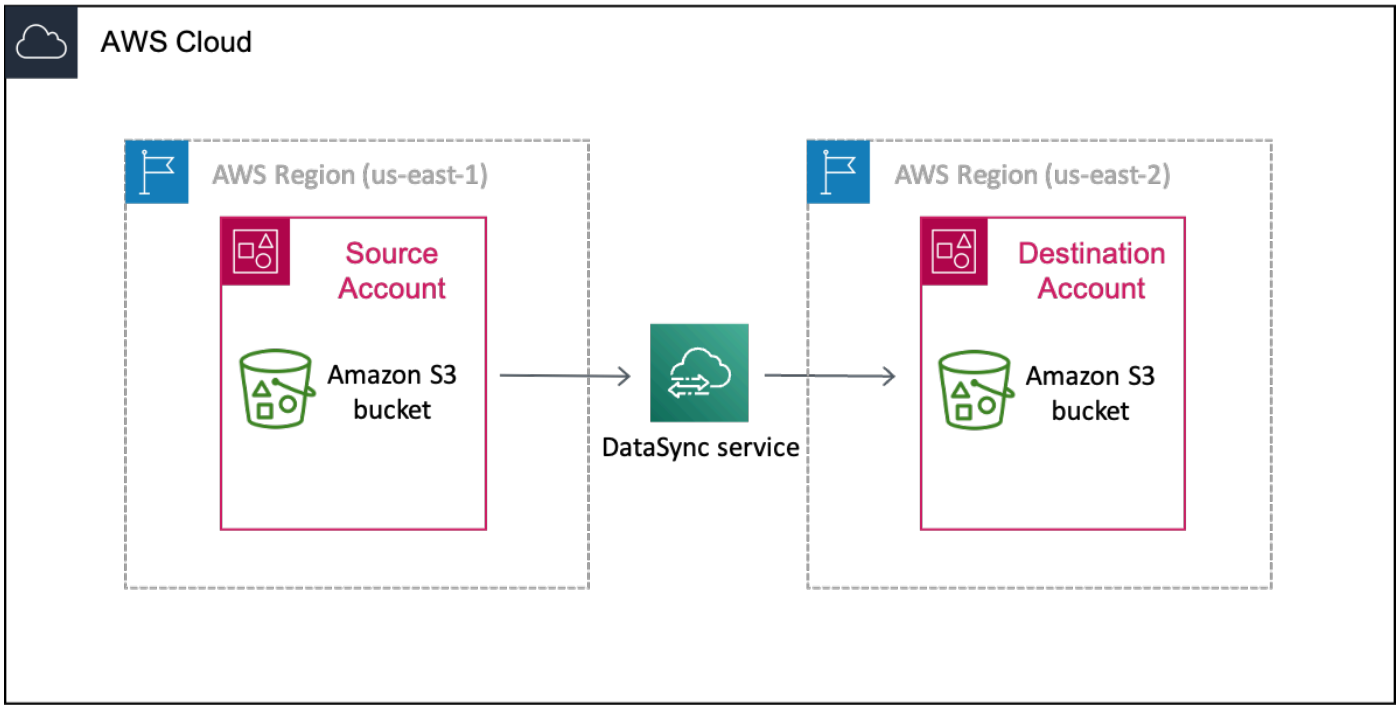
Transfers across accounts

다음 다이어그램은 서로 다른 AWS 계정에서 S3 버킷에서 다른 S3 버킷으로 데이터를 전송하는 시나리오를 보여줍니다.



Transfers across accounts and Regions

다음 다이어그램은 S3 버킷에서 다른 AWS 계정 및 리전에 있는 다른 S3 버킷으로 데이터를 전송하는 시나리오를 보여줍니다.



사전 조건: 필수 소스 계정 권한

소스의 경우 이러한 종류의 교차 계정 전송과 함께 고려해야 할 두 가지 권한 세트 AWS 계정가 있습니다.

- 사용자가 DataSync를 사용하도록 허용하는 사용자 권한(사용자 또는 스토리지 관리자일 수 있음)입니다. 이러한 권한을 통해 DataSync 위치 및 작업을 생성할 수 있습니다.
- DataSync가 대상 계정 버킷으로 데이터를 전송하도록 허용하는 DataSync 서비스 권한입니다.

소스 계정에 대한 사용자 권한

소스 계정에서 DataSync 위치 및 작업을 생성하기 위해 IAM 역할에 최소한 다음 권한을 추가합니다. 역할에 권한을 추가하는 방법에 대한 자세한 내용은 IAM 역할 생성 또는 수정을 참조하세요.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "SourceUserRolePermissions",
```

```
            "Effect": "Allow",
            "Action": [
                "datasync:CreateLocationS3",
                "datasync:CreateTask",
                "datasync:DescribeLocation*",
                "datasync:DescribeTaskExecution",
                "datasync:ListLocations",
                "datasync:ListTaskExecutions",
                "datasync:DescribeTask",
                "datasync:CancelTaskExecution",
                "datasync:ListTasks",
                "datasync:StartTaskExecution",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:ListRoles",
                "iam:CreatePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DataSync-*"
        },
        {
            "Sid": "IAMAttachRolePermissions",
            "Effect": "Allow",
            "Action": [
               "iam:AttachRolePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DataSync-*",
            "Condition": {
               "ArnLike": {
                 "iam:PolicyARN": [
                    "arn:aws:iam::111122223333:policy/DataSync-*",
                    "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
                    "arn:aws:iam::aws:policy/service-role/AWSDataSyncFullAccess"
                 ]
               }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

> **Tip**
>
> 사용자 권한을 설정하려면 AWSDataSyncFullAccess 사용을 고려하세요. 이는 사용자에게 DataSync에 대한 전체 액세스 권한과 해당 종속성에 대한 최소 액세스를 제공하는 AWS 관리형 정책입니다.

소스 계정에 대한 DataSync 서비스 권한

대상 계정 버킷으로 데이터를 전송하려면 DataSync 서비스는 소스 계정에서 다음 권한이 필요합니다.

이 자습서의 후반부에서 DataSync에 대한 IAM 역할을 생성할 때 이러한 권한을 추가합니다. 또한 대상 버킷 정책 및 DataSync 대상 위치 생성 시 이 역할(*source-datasync-role*)을 지정합니다.

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/*"
    }
  ]
}
```

사전 조건: 필수 대상 계정 권한

대상 계정에서 사용자 권한을 통해 대상 버킷의 정책을 업데이트하고 해당 액세스 제어 목록(ACL)을 비활성화할 수 있어야 합니다. 이러한 특정 권한에 대한 자세한 설명은 Amazon S3 사용자 가이드https://docs.aws.amazon.com/AmazonS3/latest/userguide/를 참조하세요.

1단계: 소스 계정에서 대상 버킷 액세스의 DataSync IAM 역할 생성

소스에는 DataSync에 대상 계정 버킷으로 데이터를 전송할 수 있는 권한을 부여하는 IAM 역할이 AWS 계정필요합니다.

계정 간에 데이터를 이전하는 것이므로 이 역할을 수동으로 생성해야 합니다. (DataSync는 동일한 계정으로 전송할 때 콘솔에서 이 역할을 생성할 수 있습니다.)

DataSync IAM 역할 생성

DataSync를 신뢰할 수 있는 엔터티로 사용하여 IAM 역할을 생성합니다.

1. 소스 계정으로 AWS Management Console 에 로그인합니다.
2. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.

3. 왼쪽 탐색 창의 액세스 관리에서 역할을 선택한 다음, 역할 생성을 선택합니다.
4. 신뢰할 수 있는 엔터티 선택 페이지에서 신뢰할 수 있는 엔터티 유형으로 AWS 서비스를 선택합니다.
5. 사용 사례로 드롭다운 목록에서 DataSync를 선택하고 DataSync를 선택합니다. 다음을 선택합니다.
6. 권한 추가 페이지에서 다음을 선택합니다.
7. 역할 이름을 제공하고 역할 생성을 선택합니다.

자세한 내용은 IAM 사용 설명서의 AWS 서비스 (콘솔)에 대한 역할 생성을 참조하세요.

DataSync IAM 역할에 권한 추가

방금 생성한 IAM 역할에는 DataSync가 대상 계정의 S3 버킷에 데이터를 전송하도록 허용하는 권한이 필요합니다.

1. IAM 콘솔의 역할 페이지에서 방금 생성한 역할을 찾아서 그 명칭을 선택합니다.
2. 역할의 세부 정보 페이지에서 권한 탭을 선택합니다. 권한 추가를 선택한 후 인라인 정책 추가를 선택합니다.
3. JSON 탭을 선택한 다음, 다음을 수행합니다.

    a. 다음 JSON을 정책 편집기에 붙여넣습니다.

> **Note**
>
> `aws:ResourceAccount`의 값은 정책에 명시된 Amazon S3 버킷을 소유한 계정의 ID여야 합니다.

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. *amzn-s3-demo-destination-bucket*의 각 인스턴스를 대상 계정의 S3 버킷의 이름으로 바꿉니다.

4. 다음을 선택합니다. 정책 명칭을 지정하고 정책 생성을 선택합니다.

2단계: 대상 계정에서 S3 버킷 정책 업데이트

대상 계정에서, 소스 계정에서 생성한 DataSync IAM 역할을 포함하도록 대상 S3 버킷 정책을 수정합니다.

시작하기 전에: 대상 계정에 필요한 권한이 있는지 확인합니다.

대상 S3 버킷 정책 업데이트

1. 에서 대상 계정으로 AWS Management Console전환합니다.
2. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
3. 왼쪽 탐색 창에서 버킷을 선택합니다.
4. 버킷 목록에서 데이터를 전송할 S3 버킷을 선택합니다.
5. 버킷의 세부 정보 페이지에서 권한 탭을 선택합니다.
6. 버킷 정책에서 편집을 선택하고 다음을 수행하여 S3 버킷 정책을 수정하세요.

   a. 편집기에 있는 내용을 업데이트하여 다음 정책 설명을 포함하세요.

      JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/source-datasync-role"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
```

```
}
```

b. 의 각 인스턴스를 소스 계정의 AWS 계정 ID*source-account*로 바꿉니다.

c. *source-datasync-role*을 소스 계정에서 DataSync용으로 생성한 IAM 역할로 바꾸세요.

d. *amzn-s3-demo-destination-bucket*의 각 인스턴스를 대상 계정의 S3 버킷의 이름으로 바꿉니다.

7. 변경 사항 저장을 선택합니다.

3단계: 대상 계정에서 S3 버킷의 ACL을 비활성화합니다.

S3 버킷으로 전송하는 모든 데이터는 대상 계정에 속해야 합니다. 이 계정이 데이터를 소유하도록 하려면 버킷의 액세스 제어 목록(ACL) 사용을 중지합니다. 자세한 설명은 Amazon S3 사용자 가이드의 객체 소유권 제어 및 버킷에 대해 ACL 사용 중지를 참조하세요.

시작하기 전에: 대상 계정에 필요한 권한이 있는지 확인합니다.

대상 S3 버킷 ACL 비활성화

1. 대상 계정으로 S3 콘솔에 로그인한 상태에서 데이터를 전송할 S3 버킷을 선택합니다.
2. 버킷의 세부 정보 페이지에서 권한 탭을 선택합니다.
3. 객체 소유권(Object Ownership)에서 편집(Edit)을 선택합니다.
4. 아직 선택하지 않은 경우, ACL 비활성화(권장) 옵션을 선택하세요.
5. 변경 사항 저장을 선택합니다.

4단계: 소스 계정에서 DataSync 위치 생성

소스 계정에서 소스 및 대상 S3 버킷을 위한 DataSync 위치를 생성합니다.

시작하기 전에: 소스 계정에 필요한 권한이 있는지 확인합니다.

DataSync 소스 위치 생성

- 소스 계정에서 데이터를 전송하려는 S3 버킷의 위치를 생성합니다.

DataSync 대상 위치 생성

소스 계정에 있는 동안 데이터를 전송하려는 S3 버킷의 위치를 생성합니다.

DataSync 콘솔 인터페이스를 사용하여 교차 계정 위치를 생성할 수 없으므로 이 지침에 따라 대상 위치를 생성하는 `create-location-s3` 명령을 실행해야 합니다. 콘솔에서 직접 시작하는 브라우저 기반 사전 인증된 AWS CloudShell쉘을 사용하여 명령을 실행하는 것이 좋습니다. CloudShell을 사용하면 AWS CLI 명령줄 도구를 다운로드하거나 설치`create-location-s3`하지 않고도와 같은 명령을 실행할 수 있습니다.

> **Note**
>
> CloudShell 이외의 명령줄 도구를 사용하여 다음 단계를 완료하려면 AWS CLI 프로필이 소스 계정에서 DataSync를 사용하는 데 필요한 사용자 권한을 포함하는 동일한 IAM 역할을 사용하는지 확인하세요.

CloudShell을 사용하여 DataSync 목적지 위치를 만들려면

1. 소스 계정에 있는 동안 다음 중 하나를 수행하여 콘솔에서 CloudShell을 시작합니다.
   - 콘솔 탐색 모음에서 CloudShell 아이콘을 선택합니다. 검색 상자 오른쪽에 있습니다.
   - 콘솔 탐색 모음의 검색 상자를 사용하여 CloudShell을 검색한 다음 CloudShell 옵션을 선택합니다.
2. 다음 `create-location-s3`명령을 복사합니다.

```
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. 대상 계정에서 *amzn-s3-demo-destination-bucket*을 S3 버킷의 이름으로 바꿉니다.
4. 대상 버킷이 소스 버킷과 다른 리전에 있는 경우 대상 버킷이 있는 리전(예: *us-east-2*)으로 *amzn-s3-demo-destination-bucket-region*을 바꿉니다. 버킷이 동일한 리전에 있는 경우 이 옵션을 제거합니다.
5. 를 소스 AWS 계정 ID*source-account-id*로 바꿉니다.
6. *source-datasync-role*을 소스 계정에서 생성한 DataSync IAM 역할로 대체하세요.
7. 명령을 CloudShell에서 실행합니다.

명령이 다음과 비슷한 DataSync 위치 ARN을 반환하면 위치가 성공적으로 생성된 것입니다.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
abcdef01234567890"
}
```

8. 왼쪽 탐색 창에서 데이터 전송을 확장한 다음 위치를 선택합니다.
9. 다른 리전에 위치를 생성한 경우 탐색 창에서 해당 리전을 선택합니다.

소스 계정에서 대상 계정 버킷용으로 방금 생성한 S3 위치를 확인할 수 있습니다.

5단계: 소스 계정에서 DataSync 전송 작업을 생성하고 시작

DataSync 작업을 시작하여 데이터를 전송하기 전에 지금까지 수행한 작업을 요약해 보겠습니다.

- 소스 계정에서 DataSync가 대상 계정의 S3 버킷에 데이터를 전송하도록 허용하는 IAM 역할을 생성했습니다.
- 대상 계정에서 DataSync가 S3 버킷으로 데이터를 전송할 수 있도록 S3 버킷을 구성했습니다.
- 소스 계정에서 전송을 위한 DataSync 소스 및 목적지 위치를 생성했습니다.

DataSync 작업을 생성하고 시작

1. 소스 계정에서 DataSync 콘솔을 계속 사용하는 동안 왼쪽 탐색 창에서 데이터 전송을 펼친 다음 작업과 작업 생성을 선택합니다.
2. 대상 계정의 버킷이 소스 계정의 버킷과 다른 리전에 있는 경우 상단 탐색 창에서 대상 버킷의 리전을 선택합니다.

> **Important**
>
> 네트워크 연결 오류를 방지하려면 대상 위치와 동일한 리전에서 DataSync 작업을 생성해야 합니다.

3. 소스 위치 구성 페이지에서 다음을 수행합니다.
   a. 기존 위치 선택을 선택합니다.
   b. (리전 간 전송의 경우) 리전 드롭다운에서 소스 버킷이 있는 리전을 선택합니다.

c. 기존 위치의 경우, 데이터를 전송할 S3 버킷의 소스 위치를 선택하고 다음을 선택합니다.

4. 대상 위치 구성 페이지에서 다음을 수행합니다.

a. 기존 위치 선택을 선택합니다.

b. 기존 위치의 경우, 데이터를 전송할 S3 버킷의 대상 위치를 선택하고 다음을 선택합니다.

5. 설정 구성 페이지에서 작업 모드를 선택합니다.

> **Tip**
>
> 확장 모드를 사용하는 것이 좋습니다. 자세한 내용은 데이터 전송을 위한 작업 모드 선택 단원을 참조하십시오.

6. 작업에 이름을 지정하고 Amazon CloudWatch 로그 그룹 지정과 같은 추가 설정을 구성합니다. 다음을 선택합니다.
7. 검토 페이지에서 설정을 검토하고 작업 생성을 선택합니다.
8. 작업의 세부 정보 페이지에서 시작을 선택하고 다음 중 하나를 선택하세요:

- 수정하지 않고 작업을 실행하려면 기본값으로 시작을 선택합니다.
- 작업을 실행하기 전에 수정하려면 재정의 옵션으로 시작을 선택합니다.

작업이 완료되면 목적지 계정의 S3 버킷을 확인합니다. 소스 계정 버킷에서 이동한 데이터를 확인할 수 있을 것입니다.

문제 해결

교차 계정 전송을 완료하는 데 문제가 발생하는 경우 다음 정보를 참조하세요.

연결 오류

서로 다른의 S3 버킷 AWS 계정 과 기본 모드 작업이 있는 리전 간에 전송할 때 DataSync 작업을 시작할 때 네트워크 연결 오류가 발생할 수 있습니다. 이 문제를 해결하려면 확장 모드 작업을 사용합니다. 또는 대상 위치와 동일한 리전에 기본 모드 작업을 생성하고 해당 작업을 실행합니다.

관련: 서버 측 암호화를 사용하여 S3 버킷으로 교차 계정 전송

서버 측 암호화를 사용하여 S3 버킷으로 이 전송을 수행하려는 경우 AWS Storage Blog에서 지침을 참조하세요.

를 사용하여 대규모 데이터 마이그레이션 수행 AWS DataSync

대규모 데이터 마이그레이션에는 다양한 형식으로 수백만 개의 파일 또는 객체를 포함하는 상당한 양의 데이터를 전송하는 작업이 포함될 수 있습니다.는 예약, 모니터링, 암호화 및 데이터 확인을 관리하여 이러한 복잡한 전송을 간소화 AWS DataSync 합니다.

대규모 데이터 마이그레이션이란 무엇인가요?

대규모 데이터 마이그레이션에는 일반적으로 다양한 소스에 분산된 테라바이트 이상의 데이터를 새 대상 스토리지 환경(이 경우 AWS)으로 전송하는 작업이 포함됩니다. 이러한 마이그레이션은 비즈니스 중단을 최소화하면서 데이터를 성공적으로 이동하기 위해 조직 내에서 신중한 계획과 조정을 거쳐야 합니다.

DataSync는 일반적으로 복잡한 이러한 마이그레이션을 단순화할 수 있습니다. 마이그레이션에 DataSync를 사용할 때 얻을 수 있는 몇 가지 이점은 다음과 같습니다.

- 고성능의 안전한 데이터 전송에 필요한 데이터 전송 프로세스 및 인프라 관리를 자동화합니다.
- 암호화 및 데이터 무결성 검증을 포함한 엔드투엔드 보안을 통해 데이터가 안전하게, 손상되지 않고, 즉시 사용할 수 있도록 보장합니다.
- 마이그레이션 속도를 높이기 위한 목적으로 특별히 구축된 네트워크 프로토콜과 병렬 다중 스레드 아키텍처입니다.

대규모 데이터 마이그레이션의 주요 단계

일반적으로 대규모 마이그레이션을 다음 단계로 나눌 수 있습니다.

- (1단계) 데이터 마이그레이션 계획 - 이 단계에서는 마이그레이션하는 이유와 작업 중인 데이터 유형을 이해합니다. 계획 활동에는 다음이 포함됩니다.
  - 마이그레이션하려는 이유 이해
  - 마이그레이션의 모든 측면을 지원하는 팀 구성
  - 데이터 위치, 형식, 사용 패턴 식별
  - 사용 가능한 하드웨어 리소스 및 네트워크 요구 사항 평가(온프레미스 데이터 센터에서 마이그레이션하는 경우)

  - DataSync를 통해 개념 증명(POC) 테스트를 실행하여 마이그레이션 타임라인 추정, 전환 기간 계획, DataSync 구성 방법 파악
- (2단계) 대규모 데이터 마이그레이션 구현 - 이 시점에서는 계획을 검증하고 마이그레이션을 시작합니다. 구현 활동에는 다음이 포함됩니다.
  - 마이그레이션 계획 검증
  - 예상대로 데이터 전송이 이루어지는지 모니터링 및 확인하는 등 단계별 전환 실행
  - 각 전환 사이에 필요에 따라 최적화 및 조정
  - 완료 후 미사용 리소스 정리

추가 리소스

AWS 권장 가이드에는 대규모 마이그레이션을 계획하고 구현하는 데 도움이 되는 다음과 같은 리소스가 있습니다. 이 가이드를 사용하여 일반적인 마이그레이션 프로세스 및 활동의 맥락에서 DataSync가 작동하는 방법을 이해합니다.

- AWS 클라우드로의 대규모 마이그레이션
- AWS 대규모 마이그레이션을 위한 전략 및 모범 사례
- AWS 대규모 마이그레이션에서 공유 파일 시스템 마이그레이션 -이 리소스에는 파일 공유 수준에서 마이그레이션을 계획하는 데 사용하고 다운로드할 수 있는 SFS-Discovery-Workbook이 포함되어 있습니다.

1단계: 대규모 데이터 마이그레이션 계획

대규모 데이터세트를 마이그레이션할 때는 계획이 필수입니다. 마이그레이션하려는 데이터, 마이그레이션 동기,가 원하는 위치에 데이터를 가져오는 AWS DataSync 데 도움이 되는 방법을 이해해야 합니다.

주제

- 마이그레이션을 위한 요구 사항 수집
- DataSync 개념 증명 실행
- 마이그레이션 타임라인 추정

마이그레이션을 위한 요구 사항 수집

대규모 데이터 마이그레이션의 첫 번째 단계에서는 조직 전체에서 다양한 정보를 수집해야 합니다.

이 정보는 마이그레이션 프로세스를 생성하는 데 도움이 되며, 대규모 마이그레이션의 경우 이는 소스에서 대상 스토리지로 작업(여러 웨이브에 걸쳐 수행)을 전환하기 위한 여러 전송 및 절차를 포함할 수 있습니다.

마이그레이션하려는 이유 이해

마이그레이션을 시작하려면 먼저 데이터를 마이그레이션 AWS하는 이유를 명확하게 이해해야 합니다. 이를 통해 기한 준수, 리소스 관리, 팀 간 조정과 같은 일반적인 마이그레이션 문제를 해결할 수 있습니다.

마이그레이션 동기를 확인하는 데 도움이 필요한 경우 다음 질문에 답하세요.

- 온프레미스 스토리지 공간을 확보하고 있나요?
- 하드웨어 지원 계약 기한을 충족하고 있나요?
- 데이터 센터 종료를 위한 것인가요?
- 마이그레이션 타임라인은 어떻게 되나요?
- 다른 클라우드 스토리지에서 데이터를 전송하고 있나요?
- 부분 또는 전체 데이터세트를 마이그레이션하고 있나요?
- 데이터 아카이브를 위한 것인가요?
- 애플리케이션 또는 사용자가 이 데이터에 정기적으로 액세스해야 하나요?

물류 파악

스토리지 환경, 마이그레이션, 조직에 대한 몇 가지 기본 물류를 다룹니다.

1. 현재 데이터 스토리지 인프라에 대한 기본적인 사항을 이해합니다.
2. DataSync 에이전트가 필요한지 확인합니다. 예를 들어 온프레미스 스토리지에서 전송하는 경우 에이전트가 필요합니다.
3. 에이전트가 필요한 경우 에이전트 요구 사항을 이해해야 합니다.

    - 에이전트는 VMware ESXi의 가상 머신(VM), Linux 커널 기반 가상 머신(KVM), Microsoft Hyper-V 하이퍼바이저로 실행할 수 있습니다. 또한 에이전트를 AWS내에서 Amazon EC2 인스턴스로 배포할 수 있습니다.

- 대규모 마이그레이션은 일반적으로 메모리 집약적입니다. 에이전트에 충분한 RAM이 있는지 확인합니다.

4. 마이그레이션에 참여해야 하는 리더십, 네트워킹, 스토리지, IT 부서의 주요 이해관계자를 파악합니다. 여기에는 다음이 포함됩니다.

   - 프로젝트와 그 결과를 전담하는 단일 스레드 리더를 찾습니다.
   - 마이그레이션하는 데이터의 소유권 및 분류를 담당하는 사용자를 파악합니다.
   - 소스를 관리하는 사용자와 마이그레이션하려는 AWS 스토리지 서비스를 관리할 사용자를 식별합니다.
   - 데이터가 들어오면 누가 데이터에 대한 다른 프로세스를 생성하고 관리할지 알아봅니다 AWS.

5. 부서 간 통신 채널을 설정합니다.
6. 비상 상황에 대한 롤백 계획을 생성합니다.
7. 웨이브, 검증, 전환 절차 등 전체 마이그레이션 프로세스를 문서화합니다. 이를 전체 마이그레이션의 런북으로 사용합니다. 마이그레이션을 계획하고 구현할 때 이 프로세스를 업데이트합니다.

마이그레이션하려는 데이터 검토

스토리지 및 애플리케이션 팀과 협력하여 마이그레이션 중인 데이터의 특성을 분석합니다. 이 정보는 DataSync로 실행할 수 있는 마이그레이션 전략을 확인하는 데 도움이 됩니다.

목차

- 데이터 사용 패턴 확인
- 데이터 구조 및 레이아웃 식별
- 공유 및 폴더 문서화
- 파일 크기 분석

데이터 사용 패턴 확인

- 자주 수정하며 적극적으로 사용하는 데이터의 경우 비즈니스 운영이 중단되지 않도록 여러 웨이브에 걸쳐 증분 전송을 계획합니다.
- 아카이브용으로 간주될 수 있는 읽기 전용 데이터의 경우 여러 웨이브에 걸쳐 진행하도록 계획할 필요가 없을 수 있습니다.

- 데이터 사용 패턴이 혼합된 경우 이러한 서로 다른 데이터세트를 별도로 마이그레이션하는 웨이브를 계획합니다. 예를 들어 아카이브 데이터에 하나의 웨이브를 계획하고, 나머지 단계는 활성 데이터 마이그레이션만을 위해 계획할 수 있습니다.

데이터 구조 및 레이아웃 식별

- 데이터가 기간(년, 월, 일) 또는 기타 패턴별로 구성되어 있는지 확인합니다.
- 이 조직 구조를 사용하여 마이그레이션 웨이브를 계획합니다. 예를 들어 하나의 웨이브로 1년 분량의 아카이브 데이터를 마이그레이션할 수 있습니다.

공유 및 폴더 문서화

- 공유 및 폴더 인벤토리를 생성합니다(각 인벤토리에 대한 파일 또는 객체 수 포함).
- 활성 데이터세트가 있는 공유 및 폴더를 식별합니다. 마이그레이션 과정에서 증분 전송이 필요할 수 있습니다.
- DataSync 할당량을 검토합니다. 이는 DataSync 구성 시 데이터세트 분할 방법을 계획하는 데 도움이 될 수 있습니다.

파일 크기 분석

- 더 큰 파일(MB 또는 GB)을 전송하는 경우 더 작은 파일(KB)을 전송할 때에 비해 데이터 처리량이 더 높을 것으로 예상됩니다.
- 더 작은 파일을 많이 사용하는 경우 스토리지 시스템에 더 많은 메타데이터 작업이 필요하고 데이터 처리량이 더 낮을 것으로 예상됩니다. DataSync는 소스 및 대상 위치를 비교하고 확인할 때 이러한 작업을 수행합니다.

스토리지 요구 사항 식별

호환되는 AWS 스토리지 서비스를 선택하여 데이터를 마이그레이션하려면 소스 스토리지 시스템의 특성과 성능을 평가해야 합니다.

또한 이 정보는 마이그레이션 과정에서 비즈니스 운영에 미치는 영향을 최소화하기 위해 전송을 예약하는 데 도움이 될 수 있습니다.

목차

- 소스 스토리지 지원 확인

- 메타데이터 보존 요구 사항 검토
- 소스 스토리지에서 성능 지표 수집
- 대상 AWS 스토리지 서비스 선택

소스 스토리지 지원 확인

DataSync는 NFS, SMB, HDFS, S3 호환 객체 스토리지 클라이언트를 통해 액세스할 수 있는 다양한 스토리지 시스템에서 작동할 수 있습니다.

다른 클라우드 스토리지에서 마이그레이션하는 경우 DataSync가 해당 공급자와 함께 작동할 수 있는지 확인합니다. 지원하는 소스 목록은 데이터를 어디로 전송할 수 있나요 AWS DataSync?을(를) 참조하세요.

메타데이터 보존 요구 사항 검토

DataSync는 전송 과정에서 파일 또는 객체 메타데이터를 보존할 수 있습니다. 메타데이터 보존 방법은 전송 위치와 해당 위치에서 유사한 유형의 메타데이터를 사용하는지 여부에 따라 달라집니다.

DataSync는 경우에 따라 NTFS 임의 액세스 목록(DACL)과 같은 파일 메타데이터를 보존하기 위해 추가 권한이 필요합니다.

자세한 내용은 DataSync가 파일 및 객체 메타데이터를 처리하는 방법 이해 단원을 참조하십시오.

소스 스토리지에서 성능 지표 수집

소스 스토리지의 평균 및 피크 워크로드 기간 동안 기준 IOPS 및 디스크 처리량을 측정합니다. 데이터를 전송하면 소스 및 대상 스토리지 시스템 모두에 I/O 오버헤드가 추가됩니다.

이 성능 데이터를 스토리지 시스템의 사양과 비교하여 사용 가능한 성능 리소스를 확인합니다.

대상 AWS 스토리지 서비스 선택

이 시점에서 데이터에 적합한 AWS 스토리지 서비스가 무엇인지 알고 있을 수 있습니다. 그렇지 않다면 데이터 사용 패턴과 스토리지 성능은 결정 시 고려해야 할 몇 가지 영역입니다. 예를 들어, 아카이브 데이터가 있다면 Amazon S3를, 활성 데이터에 대해서는 Amazon FSx 또는 Amazon EFS를 고려할 수 있습니다.

데이터에 적합한 객체 또는 파일 기반 스토리지를 결정하는 데 도움이 필요하면 AWS 스토리지 서비스 선택을 참조하세요.

네트워크 요구 사항 확인

DataSync로 데이터를 마이그레이션하려면 소스 스토리지, 에이전트 및 간에 네트워크 연결을 설정해야 합니다 AWS. 또한 충분한 네트워크 대역폭과 인프라를 계획해야 합니다.

네트워크 엔지니어 및 스토리지 관리자와 협력하여 다음 네트워크 요구 사항을 수집합니다.

목차

- 사용 가능한 네트워크 대역폭 평가
- 네트워크를에 연결하기 위한 옵션 고려 AWS
- 에이전트 통신을 위한 서비스 엔드포인트 선택
- 충분한 네트워크 인프라 확보 계획

사용 가능한 네트워크 대역폭 평가

사용 가능한 네트워크 대역폭은 전송 속도와 전체 마이그레이션 시간에 영향을 미칩니다. 온프레미스 스토리지 시스템에서 전송하는 경우 다음을 수행합니다.

- 네트워크 팀과 협력하여 평균 및 최대 대역폭 사용률을 결정합니다.
- 데이터 전송 가능 기간을 파악하여 일상 작업이 중단되지 않도록 합니다. 그러면 마이그레이션 웨이브와 전환이 언제 발생하는지 알 수 있습니다.

DataSync가 사용하는 대역폭의 양을 제어할 수 있습니다. 자세한 내용은 AWS DataSync 작업에 대한 대역폭 제한 설정 단원을 참조하십시오.

다른 클라우드 스토리지에서 전송은 일반적으로 퍼블릭 인터넷을 통해 이루어지므로 이러한 전송에는 일반적으로 대역폭 제한 및 고려 사항이 적습니다.

네트워크를에 연결하기 위한 옵션 고려 AWS

DataSync 전송을 위한 네트워크 연결을 설정하려면 다음 옵션을 고려하세요.

- Direct Connect - DataSync와 함께 Direct Connect를 사용하기 위한 아키텍처 및 라우팅 예시를 검토합니다. Amazon CloudWatch를 사용하여 Direct Connect 활동을 모니터링할 수 있습니다.
- VPN - AWS Site-to-Site VPN은 터널당 최대 1.25Gbps의 처리량을 제공합니다.
- 퍼블릭 인터넷 - 네트워크 사용 데이터에 대해서는 인터넷 서비스 공급자에게 문의하세요.

에이전트 통신을 위한 서비스 엔드포인트 선택

DataSync 에이전트는 서비스 엔드포인트를 사용하여 DataSync 서비스와 통신합니다. 사용하는 엔드포인트 유형은 네트워크에 대해 AWS에 연결하는 방법에 따라 달라집니다.

충분한 네트워크 인프라 확보 계획

생성하는 모든 전송 작업에 대해 DataSync는 데이터 전송을 위한 네트워크 인프라를 자동으로 생성하고 관리합니다. 이 인프라를 네트워크 인터페이스 또는 탄력적 네트워크 인터페이스라고 하며, 이는 가상 네트워크 카드를 나타내는 Amazon 가상 프라이빗 클라우드(VPC)의 논리적 네트워킹 구성 요소입니다. 자세한 내용은 Amazon EC2 사용 설명서를 참조하세요.

각 네트워크 인터페이스는 대상 VPC 서브넷에서 단일 IP 주소를 사용합니다. 마이그레이션에 충분한 네트워크 인프라가 있는지 확인하려면 다음을 수행합니다.

- DataSync가 사용자의 DataSync 대상 위치에 생성한 네트워크 인터페이스 수에 주목합니다.
- 서브넷에 DataSync 작업에 필요한 충분한 IP 주소가 있는지 확인하세요. 예를 들어 에이전트를 사용하는 작업에는 4개의 IP 주소가 필요합니다. 마이그레이션을 위해 4개의 작업을 생성하는 경우 서브넷에 사용 가능한 IP 주소 16개가 필요합니다.

DataSync 개념 증명 실행

를 사용하여 개념 증명(POC)을 실행하면 데이터 마이그레이션 계획의 다음 측면을 검증하는 AWS DataSync 데 도움이 됩니다.

- 소스 위치와 대상 위치 간의 네트워크 연결을 확인합니다.
- 초기 DataSync 작업 구성을 검증합니다.
- 데이터 전송 성능을 측정합니다.
- 마이그레이션 타임라인을 추정합니다.
- 마이그레이션 작업을 진행하는 주요 이해관계자와 함께 성공 기준을 정의합니다.

개념 증명 시작하기

1. DataSync 에이전트 생성:
    1. 에이전트를 배포합니다.
    2. 에이전트용 서비스 엔드포인트를 선택합니다.
    3. 에이전트 활성화.

4. 에이전트의 네트워크 연결을 확인합니다.

2. 마이그레이션할 데이터를 대표하는 데이터의 작은 하위 집합을 선택합니다.

   예를 들어, 소스 스토리지에 용량이 큰 파일과 작은 파일이 혼합되어 있는 경우 POC에서 전송하는 데이터의 하위 집합도 이러한 특성을 반영해야 합니다. 이를 통해 스토리지 시스템, 네트워크, DataSync의 성능을 예비적으로 이해할 수 있습니다.

3. 온프레미스 또는 기타 클라우드 스토리지 시스템에 대한 DataSync 소스 위치를 생성합니다.
4. AWS 스토리지 서비스의 DataSync 대상 위치를 생성합니다.
5. 데이터 하위 집합만 전송하는 필터를 사용하여 DataSync 전송 작업을 생성합니다.
6. DataSync 작업을 시작합니다.
7. 다음을 모니터링하여 전송 성능 지표를 수집합니다.

   - 작업 실행에 대한 데이터 및 파일 처리량입니다. DataSync 콘솔 또는 DescribeTaskExecution 작업을 통해이를 수행할 수 있습니다. `DescribeTaskExecution`을 사용하는 경우 이러한 지표를 계산하는 방법은 다음과 같습니다.
     - 데이터 처리량: `BytesWritten`를 `TransferDuration`으로 나누기
     - 파일 처리량: `FilesTransferred`을 `TransferDuration`으로 나누기
   - 소스 및 대상 스토리지 사용률입니다. 스토리지 관리자와 긴밀히 협력하여 이 정보를 얻습니다.
   - 네트워크 사용량입니다.

8. 대상 위치에서 전송된 데이터를 확인합니다.

   - CloudWatch Logs 에서 작업 실행 오류를 검토합니다.
   - 대상 위치에 권한과 메타데이터가 보존되어 있는지 확인합니다.
   - 애플리케이션과 사용자가 예상대로 대상 데이터에 액세스할 수 있는지 확인합니다.
   - 발생하는 모든 문제를 해결합니다. 자세한 내용은 AWS DataSync 문제 해결 단원을 참조하십시오.

9. 작업을 몇 번 더 실행하여 DataSync가 데이터를 준비, 전송, 확인하는 데 걸리는 시간을 파악할 수 있습니다. (자세한 내용은 태스크 실행 상태 섹션을 참조하세요.)

   작업을 두 번 이상 실행하면 DataSync는 기본적으로 증분 전송을 수행하고 이전 작업 실행에서 변경된 데이터만 복사합니다.

   전송 시간의 경우 증분 전송이 더 짧을 수 있지만, DataSync는 항상 위치를 스캔하고 비교하여 전송할 대상을 식별하여 동일한 방식으로 전송을 준비합니다. 이러한 준비 시간을 사용하여 마이그레이션의 전환 타임라인을 추정할 수 있습니다.

10. 필요한 경우 POC 중에 학습한 내용을 기반으로 마이그레이션 계획을 업데이트합니다.

마이그레이션 타임라인 추정

지금까지 수집한 정보를 바탕으로 AWS DataSync사용 시 마이그레이션에 걸리는 시간을 추정할 수 있습니다.

데이터 전송 타임라인 추정

마이그레이션 요구 사항 수집 중에 수집한 다음 정보와 DataSync 개념 증명(POC)을 기반으로 DataSync가 데이터를 전송하는 데 걸리는 시간을 추정할 수 있습니다.

- 사용 가능한 네트워크 대역폭
- 소스 및 대상 스토리지 사용률 지표
- DataSync POC의 성능 지표

데이터 전송 타임라인을 추정하는 방법

1. POC의 데이터 및 파일 처리량을 사용 가능한 네트워크 대역폭과 비교합니다.
2. 처리량이 사용 가능한 대역폭보다 낮은 경우(예: 네트워크 대역폭이 10Gbps이고 처리량이 300MiB/s인 경우) 데이터세트를 여러 작업으로 파티셔닝하여 대역폭 사용을 극대화하는 것이 좋습니다.

   DataSync에는 데이터세트를 파티셔닝하는 몇 가지 옵션이 있습니다. 자세한 내용은 데이터 파티셔닝을 사용하여 마이그레이션 가속화 단원을 참조하십시오.
3. 이론적 최소 전송 시간을 제공하는 다음 공식을 사용하여 전송에 걸리는 일수를 계산합니다.

   ```
   (DATA_SIZE * 8 bits per byte)/(CIRCUIT * NETWORK_UTILIZATION percentage * 3600
    seconds per hour * AVAILABLE_HOURS) = Number of days
   ```

   이 공식을 사용할 때는 다음을 고유한 값으로 변경합니다.

   - `DATA_SIZE`: 마이그레이션하려는 데이터의 양입니다(바이트로 표시).
   - `CIRCUIT`: 사용 가능한 네트워크 대역폭입니다(초당 비트로 표시).
   - `NETWORK_UTILIZATION`: 사용 중인 네트워크의 백분율입니다.
   - `AVAILABLE_HOURS`: 매일 이용 가능한 작업 시간입니다.

예를 들어, 다음과 같이 100TB의 데이터, 1Gbps 인터넷 연결, 80% 네트워크 사용률, 하루 24시간 가용성이 있는 마이그레이션을 계산할 수 있습니다.

```
(100,000,000,000,000 bytes * 8) / (1,000,000,000 bps * 0.80 * 3600 *
24) = 11.57 days
```

이 경우 실제 환경을 고려하지 않았을 때 마이그레이션은 거의 12일이 걸립니다.

4. 실제 조건을 고려하여 계산된 전송 기간을 조정합니다.

   - 네트워크 성능 변동
   - 스토리지 성능 변형
   - 마이그레이션 웨이브 간 가동 중지 시간

전환 타임라인 추정

활성 데이터세트를 마이그레이션하는 경우 비즈니스 운영을 중단하지 않기 위해 전환이 필요할 수 있습니다.

전환에 걸리는 시간을 과소평가하지 마세요. 대규모 마이그레이션에서 전환 활동이 전체 마이그레이션 시간의 최대 30%를 차지하는 일은 흔히 일어납니다.

1. 증분 변경 사항을 스캔하는 데이터의 양을 줄이기 위해 여러 웨이브에서 전환을 수행해야 하는지 평가합니다.

   이를 위해 공유, 폴더, 스토리지 시스템을 기반으로 파티셔닝한 데이터세트를 전환하는 전략을 수행할 수 있습니다.

2. DataSync가 POC 중에 데이터를 준비, 전송, 확인하는 데 일반적으로 얼마나 걸렸는지 검토합니다.

   특히 작업 실행 준비에 걸린 기간에 주목합니다. 이 정보를 찾으려면 DescribeTaskExecution 작업을 실행한 다음 지속 시간(밀리초) 동안의 PrepareDuration 값을 확인합니다.

3. 병렬 작업의 시간 델타를 측정하여 전환에 걸리는 시간을 추정합니다.

   병렬 작업에 대한 자세한 내용은 데이터 파티셔닝을 사용하여 마이그레이션 가속화을(를) 참조하세요.

4. 전환 추정을 사용하여 전환 일정을 예약합니다. 본질적으로 이는 소스 데이터를 수정할 수 없는 유지 관리 기간입니다.

다음 단계

타임라인을 추정하고 나면 마이그레이션 구현을 시작할 준비가 끝납니다.

2단계: 대규모 데이터 마이그레이션 구현

계획 중에 수집한 정보를 사용하여 AWS DataSync 를 사용하여 새 스토리지 시스템으로 마이그레이션할 수 있습니다. 아직 이를 수행하지 않은 경우 대규모 마이그레이션을 위한AWS 권장 가이드 리소스를 검토하는 것이 좋습니다.

주제

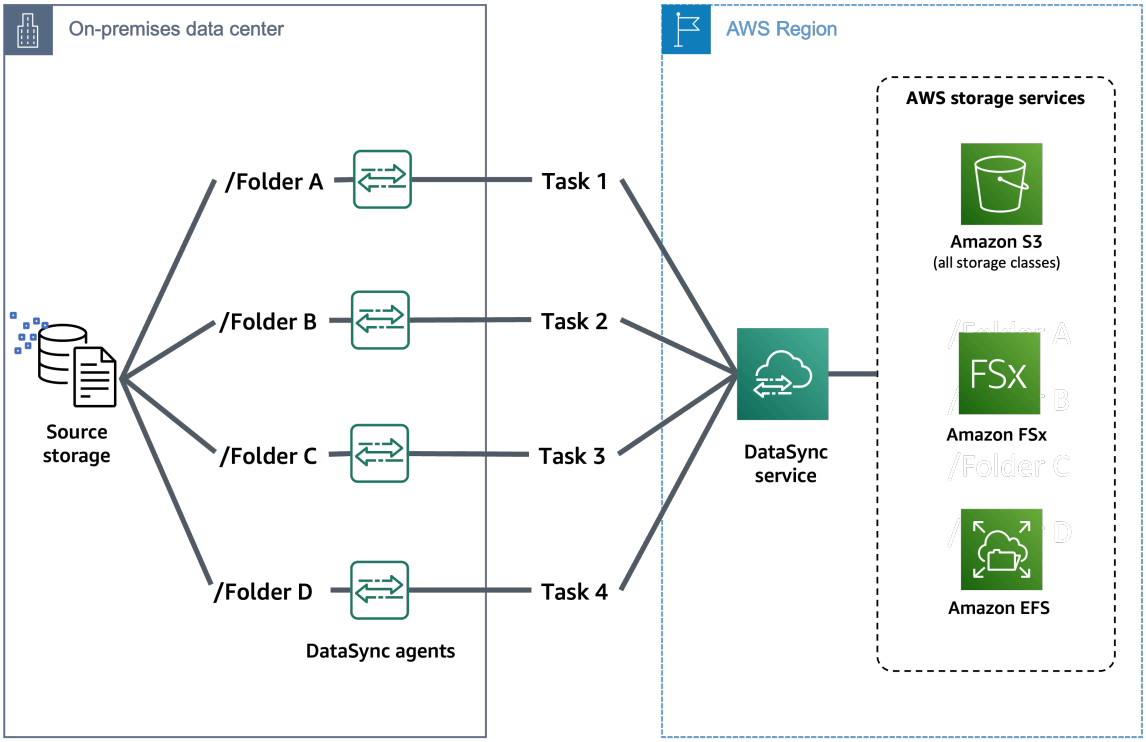
- 데이터 파티셔닝을 사용하여 마이그레이션 가속화
- DataSync 전송 작업 실행
- 전송 모니터링

데이터 파티셔닝을 사용하여 마이그레이션 가속화

대규모 마이그레이션의 경우 데이터세트를 여러 DataSync 작업으로 파티셔닝하는 것이 좋습니다. 소스 데이터를 여러 작업(필요한 경우 에이전트)으로 분할하면 전송을 병렬로 처리하고 마이그레이션 타임라인을 줄일 수 있습니다.

파티셔닝은 DataSync 할당량 내에서 작업의 모니터링 및 디버깅을 간소화하는 데도 도움이 됩니다.

다음 다이어그램은 여러 DataSync 작업 및 에이전트를 사용하여 동일한 소스 스토리지 위치에서 데이터를 전송하는 방법을 보여줍니다. 이 시나리오에서 각 작업은 소스 위치의 특정 폴더를 대상으로 합니다. 이러한 접근 방식에 대한 자세한 내용과 예제는 AWS DataSync 스케일 아웃 아키텍처를 사용하여 데이터 전송을 가속화하는 방법을 참조하세요.



폴더 또는 접두사별로 데이터세트 파티셔닝

DataSync 소스 위치 생성 시 DataSync가 읽을 폴더, 디렉터리, 접두사를 지정할 수 있습니다. 예를 들어 최상위 디렉터리가 있는 파일 공유를 마이그레이션하는 경우 다른 디렉터리 경로를 지정하여 여러 위치를 생성할 수 있습니다. 그런 다음 이러한 위치를 사용하여 마이그레이션 중에 여러 DataSync 작업을 실행할 수 있습니다.

필터를 사용하여 데이터세트 파티셔닝

전송 시 필터를 적용하여 소스 위치의 데이터를 포함하거나 제외할 수 있습니다. 대규모 마이그레이션 맥락에서 필터는 데이터세트의 특정 부분으로 작업 범위를 지정하는 데 도움이 될 수 있습니다.

예를 들어 연도별로 구성된 아카이브 데이터를 마이그레이션하는 경우 특정 연도 또는 여러 연도에 일치하는 포함 필터를 생성할 수 있습니다. 작업을 실행할 때마다 다른 연도와 일치하도록 필터를 수정할 수도 있습니다.

매니페스트를 사용하여 데이터세트 파티셔닝

매니페스트는 DataSync가 전송하려는 파일 또는 객체의 목록입니다. 매니페스트를 사용하면 DataSync가 전송할 대상을 결정하기 위해 소스 위치의 모든 데이터를 읽을 필요가 없습니다.

소스 스토리지의 인벤토리에서 또는 이벤트 기반 접근 방식을 통해 매니페스트를 생성할 수 있습니다(예: 수억 개의 객체 AWS DataSync 로 구현 참조). 작업을 시작할 때마다 다른 매니페스트를 사용하면, 같은 작업을 통해 다양한 데이터세트를 전송할 수 있습니다.

DataSync 전송 작업 실행

각 마이그레이션 웨이브 동안 데이터 전송은 대부분 같은 일반 프로세스를 따릅니다.

1. 데이터에 대한 초기 전체 전송을 실행합니다.
2. 대상의 데이터를 확인합니다.
3. 초기 전송 이후 변경되었을 수 있는 모든 데이터에 대해 증분 전송을 실행합니다.
4. 작업을 대상 위치로 전환합니다.
5. 전환 결과를 검토합니다.

작업 실행

전체 마이그레이션 시간을 최소화하려면 업무 시간 중에 DataSync 전송 작업을 실행해야 할 수 있습니다. 이러한 상황에서는 초기 전체 전송을 실행한 다음 사용자 및 애플리케이션으로 인해 소스 위치에서 발생한 변경을 반영하는 증분 전송을 실행하는 것이 일반적입니다.

업무 시간 동안 네트워크 관련 문제를 방지하려면 작업에서 사용하는 대역폭의 양을 제한할 수 있습니다. 자세한 내용은 AWS DataSync 작업에 대한 대역폭 제한 설정 단원을 참조하십시오.

1. 초기 전체 전송을 실행합니다.
   a. DataSync 작업을 시작(병렬로 작업을 실행하는 경우 여러 작업을 시작)합니다.
   b. 작업 실행의 진행 상황과 성능을 모니터링합니다.
   c. 데이터가 예상대로 전송되었는지 확인합니다(예: 파일 메타데이터가 보존되었는지).
2. 증분 전송 실행:
   a. 작업을 예약하여 주기적으로 실행하도록 설정합니다.
   b. 작업 실행을 모니터링하고 오류가 발생하면 수정합니다.

전환 수행

초기 및 증분 전송 후 대상 위치로 작업을 전환하는 프로세스를 시작할 수 있습니다.

1. 예약된 유지 관리 기간을 시작합니다.
2. 애플리케이션 및 사용자에 대해 소스 스토리지 시스템을 읽기 전용으로 업데이트합니다.
3. 최종 증분 전송을 실행하여 소스 위치와 대상 위치 간에 남아 있는 델타를 복사합니다.
4. 철저한 데이터 검증을 수행합니다(예: CloudWatch Logs 및 작업 보고서 검토).
5. 애플리케이션과 사용자를 대상 위치의 새 환경으로 전환합니다.
6. 애플리케이션 기능을 테스트하고 사용자가 대상 위치의 데이터에 액세스할 수 있는지 확인합니다.
7. 마이그레이션 팀과 전송 결과를 검토하기 위한 회고 회의 일정을 예약합니다. 다음 예시와 같은 탐색 질문을 제시합니다.
   - 전환에 성공했나요? 실패했다면 어떤 문제가 있었나요?
   - 사용 가능한 모든 대역폭을 사용했나요?
   - 소스 및 대상 스토리지가 완전히 활용되었나요?
   - 추가 작업으로 더 많은 데이터 처리량을 확보할 수 있나요?
   - 유지 관리 기간을 더 길게 계획해야 하나요?
8. 필요한 경우 다음 단계를 시작하기 전에 마이그레이션 계획을 업데이트합니다.

전송 모니터링

AWS DataSync 는 전송을 검증하고 디버깅하는 데 도움이 되는 몇 가지 모니터링 옵션을 제공합니다.

CloudWatch 지표를 사용하여 전송 모니터링

DataSync 작업 실행의 지표를 사용하여 사용자 지정 CloudWatch 대시보드를 생성할 수 있습니다. 자세한 내용은 Amazon CloudWatch 지표를 사용한 데이터 전송 모니터링 단원을 참조하십시오.

태스크 리포트로 이체 모니터링

수백만 개의 파일 또는 객체를 전송하는 경우 작업 보고서 사용을 고려하세요. 작업 보고서는 작업 실행 중에 DataSync가 전송, 건너뛰기, 확인, 삭제하려는 항목에 대한 자세한 정보를 제공합니다. 자세한 내용은 작업 보고서로 데이터 전송 모니터링 단원을 참조하십시오.

AWS Glue, Amazon Athena 및 Amazon Quick과 같은 AWS 서비스를 사용하여 작업 보고서를 시각화할 수도 있습니다. 자세한 내용은 AWS 스토리지 블로그를 참조하세요.

CloudWatch Logs를 사용하여 전송 모니터링

최소한 기본 정보를 기록하고 오류를 전송하도록 작업을 구성하는 것이 좋습니다. 자세한 내용은 단원을 참조하십시오Amazon CloudWatch Logs를 사용한 데이터 전송 모니터링.

AWS DataSync API

AWS Management Console 및 외에도 AWS DataSync API를 사용하여 SDK로 DataSync를 구성하고 관리할 AWS CLI수 있습니다. AWS SDKs

주제

- 작업
- 데이터 타입
- 일반적인 오류 유형
- 공통 파라미터

작업

다음 작업이 지원됩니다.

- 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

진행 중인 AWS DataSync 작업 실행을 중지합니다. 일부 파일의 전송이 갑자기 중단되었습니다. 대상으로 전송된 파일 콘텐츠가 불완전하거나 원본 파일과 일치하지 않을 수 있습니다.

하지만 동일한 작업을 사용하여 새 작업 실행을 시작하고 완료하도록 허용하면 대상의 파일 콘텐츠가 완전하고 일관되게 유지됩니다. 이는 작업 실행을 방해하는 다른 예상치 못한 오류에도 적용됩니다. 이러한 모든 경우에 DataSync는 다음 작업 실행 시작 시 전송을 성공적으로 완료합니다.

구문 요청

```
{
   "TaskExecutionArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

TaskExecutionArn

중지할 작업 실행의 Amazon 리소스 이름(ARN) 입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

필수 여부: 예

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateAgent

스토리지 환경에 배포하는 AWS DataSync 에이전트를 활성화합니다. 활성화 프로세스는 에이전트를 와 연결합니다 AWS 계정.

아직 에이전트를 배포하지 않은 경우 Do I need a DataSync agent? 섹션을 참조하세요.

구문 요청

```
{
   "ActivationKey": "string",
   "AgentName": "string",
   "SecurityGroupArns": [ "string" ],
   "SubnetArns": [ "string" ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "VpcEndpointId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

ActivationKey

사용자 DataSync 에이전트의 활성화 키를 지정합니다. 활성화 키가 없는 경우 에이전트 활성화를 참조하세요.

유형: 문자열

길이 제약 조건: 최대 길이는 29.

패턴: `[A-Z0-9]{5}(-[A-Z0-9]{5}){4}`

필수 여부: 예

AgentName

사용자 에이전트의 이름을 지정합니다. 기억할 수 있는 이름을 지정하는 것이 좋습니다.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

SecurityGroupArns

에이전트와 VPC 서비스 엔드포인트 간의 트래픽을 허용하는 보안 그룹의 Amazon 리소스 이름(ARN)을 지정합니다. 하나의 ARN만 지정할 수 있습니다.

유형: 문자열 배열

배열 멤버: 고정된 항목 수는 1개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

필수 여부: 아니요

SubnetArns

VPC 서비스 엔드포인트가 위치한 서브넷의 ARN을 지정합니다. 하나의 ARN만 지정할 수 있습니다.

유형: 문자열 배열

배열 멤버: 고정된 항목 수는 1개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/subnet-[a-f0-9]+$`

필수 여부: 아니요

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 에이전트에 대한 태그를 적어도 하나 이상 만드는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

VpcEndpointId

사용 중인 VPC 서비스 엔드포인트의 ID를 지정합니다. 예를 들어 VPC 엔드포인트 ID는 `vpce-01234d5aff67890e1`과 같습니다.

> **Important**
>
> 사용하는 VPC 서비스 엔드포인트에는 DataSync 서비스 이름(예: `com.amazonaws.us-east-2.datasync`)이 포함되어야 합니다.

유형: String

패턴: `^vpce-[0-9a-f]{17}$`

필수 여부: 아니요

응답 구문

```
{
   "AgentArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AgentArn

방금 활성화한 에이전트의 ARN. ListAgents 작업을 사용하여 AWS 계정 및의 에이전트 목록을 반환합니다 AWS 리전.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

다음 예제는 DataSync 에이전트를 활성화합니다.

```
{
    "ActivationKey": "AAAAA-1AAAA-BB1CC-33333-EEEEE",
    "AgentName": "MyAgent",
    "Tags": [{
        "Key": "Job",
        "Value": "TransferJob-1"
    }]
```

```
}
```

샘플 응답

응답은 활성화된 에이전트의 ARN을 반환합니다.

```
{
    "AgentArn": "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44baca3"
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationAzureBlob

Microsoft Azure Blob 스토리지 컨테이너의 전송 위치를 생성합니다.이 위치를 전송 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다. 컨테이너에 연결하는 DataSync 에이전트를 사용하거나 사용하지 않고 전송할 수 있습니다.

시작하기 전에 DataSync가 Azure Blob Storage에 액세스하는 방법과 액세스 계층 및 Blob 유형을 처리하는 방법을 알고 있어야 합니다.

구문 요청

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

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccessTier

객체 또는 파일이 전송되어야 할 액세스 계층을 지정합니다. 이는 해당 위치를 전송 대상으로 사용하는 경우에만 적용됩니다. 자세한 내용은 액세스 티어를 참조하세요.

타입: 문자열

유효 값: `HOT | COOL | ARCHIVE`

필수 여부: 아니요

AgentArns

(선택 사항) 사용자 Azure Blob 스토리지 컨테이너와 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)을 지정합니다. 에이전트 없는 클라우드 간 전송을 설정하는 경우 이 파라미터에 값을 지정할 필요가 없습니다.

하나 이상의 에이전트를 지정할 수 있습니다. 자세한 내용은 전송에 복수 에이전트 사용을 참조하세요.

> **Note**
>
> 스토리지 위치를 처음 생성할 때 이 파라미터를 올바르게 구성해야 합니다. 에이전트를 생성한 후에는 스토리지 위치에서 에이전트를 추가하거나 제거할 수 없습니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

AuthenticationType

DataSync가 Azure Blob Storage에 액세스하는 데 사용하는 인증 방법을 지정합니다. DataSync는 공유 액세스 서명(SAS)을 사용하여 블롭 스토리지에 액세스할 수 있습니다.

타입: 문자열

유효 값: SAS | NONE

필수 사항 여부: 예

BlobType

개체 또는 파일을 Azure Blob Storage로 전송할 때 사용할 블롭 유형을 지정합니다. 현재 DataSync는 데이터를 블록으로 Azure Blob Storage로 이동하는 것만 지원합니다. 블롭 유형에 대한 자세한 내용은 Azure Blob Storage 설명서를 참조하세요.

타입: 문자열

유효 값: BLOCK

필수 여부: 아니요

CmkSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 지정합니다. 이는 DataSync가 고객 관리형 AWS KMS key와 함께 특정 AzureBlob 스토리지 위치에 액세스하는 데 사용하는 인증 토큰을 포함합니다.

이 파라미터를 CreateLocationAzureBlob 요청의 일부로 포함하는 경우 KMS 키 ARN만 제공합니다. DataSync는 이 KMS 키를 SasConfiguration에 지정한 인증 토큰과 함께 사용하여 DataSync 관리형 보안 암호를 생성하고 위치 액세스 자격 증명을 저장합니다.

DataSync에 지정한 KMS 키에 액세스할 수 있는 권한이 있는지 확인합니다. 자세한 내용은 사용자 지정으로 암호화된 서비스 관리형 보안 암호 사용을 참조하세요 AWS KMS key.

> **Note**
>
> CmkSecretConfig(SasConfiguration 포함) 또는 CustomSecretConfig(SasConfiguration 제외)을 사용하여 CreateLocationAzureBlob 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CmkSecretConfig객체

필수 여부: 아니요

ContainerUrl

전송과 관련된 Azure Blob 저장소 컨테이너의 URL을 지정합니다.

유형: 문자열

길이 제약 조건: 최대 길이는 325입니다.

패턴: `^https:\/\/[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}\/[a-z0-9](-?[a-z0-9]){2,62}$`

필수 여부: 예

CustomSecretConfig

AzureBlob 스토리지 위치의 인증 토큰이 Secrets Manager에 일반 텍스트로 저장되는 고객 관리형 Secrets Manager 보안 암호의 구성 정보를 지정합니다. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다. 자세한 내용은 관리하는 보안 암호 사용을 참조하세요.

> **Note**
>
> `CmkSecretConfig`(`SasConfiguration` 포함) 또는 `CustomSecretConfig`(`SasConfiguration` 제외)을 사용하여 `CreateLocationAzureBlob` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CustomSecretConfig객체

필수 여부: 아니요

SasConfiguration

DataSync가 Azure Blob Storage에 액세스할 수 있도록 허용하는 SAS 구성을 지정합니다.

> **Note**
>
> `SasConfiguration`을 사용하여 인증 토큰을 제공하지만 `CmkSecretConfig` 또는 `CustomSecretConfig`을 사용하여 보안 암호 구성 세부 정보를 제공하지 않는 경우, DataSync는 AWS 계정의 Secrets Manager 보안 암호를 사용하여 토큰을 저장합니다.

유형: AzureBlobSasConfiguration객체

필수 여부: 아니요

Subdirectory

컨테이너의 가상 디렉터리로의 전송을 제한하려는 경우(예:/my/images) 경로 세그먼트를 지정합니다.

유형: 문자열

길이 제약: 최대 길이 1024.

패턴: ^[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}\p{C}]*$

필수 여부: 아니요

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 전송 위치에 대한 이름 태그를 적어도 하나 작성하는 것이 좋습니다.

유형: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

생성한 Azure Blob 저장소 전송 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationEfs

Amazon EFS 파일 시스템의 전송 위치를 생성합니다. AWS DataSync 는 이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 수 있습니다.

시작하려면 먼저 DataSync에서 Amazon EFS 파일 시스템에 액세스하는 방법을 이해해야 합니다.

구문 요청

```
{
   "AccessPointArn": "string",
   "Ec2Config": {
      "SecurityGroupArns": [ "string" ],
      "SubnetArn": "string"
   },
   "EfsFilesystemArn": "string",
   "FileSystemAccessRoleArn": "string",
   "InTransitEncryption": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccessPointArn

DataSync가 Amazon EFS 파일 시스템을 탑재하는 데 사용하는 액세스 포인트의 Amazon 리소스 이름(ARN)을 지정합니다.

자세한 내용은 Accessing restricted file systems 섹션을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

필수 여부: 아니요

Ec2Config

DataSync가 Amazon EFS 파일 시스템의 탑재 대상 중 하나에 연결하는 데 사용하는 서브넷 및 보안 그룹을 지정합니다.

타입: Ec2Config객체

필수 항목 여부: 예

EfsFilesystemArn

Amazon EFS 파일 시스템에 대한 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]{8,40}$`

필수 여부: 예

FileSystemAccessRoleArn

DataSync가 Amazon EFS 파일 시스템에 액세스할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할을 지정합니다.

이 역할 생성에 대한 자세한 내용은 Creating a DataSync IAM role for file system access 섹션을 참조하세요.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

필수 여부: 아니요

InTransitEncryption

DataSync가 Amazon EFS 파일 시스템으로 또는 파일 시스템에서 데이터를 전송할 때 Transport Layer Security(TLS) 1.2 암호화를 사용할지 여부를 지정합니다.

`AccessPointArn`을 사용하여 액세스 지점을 지정하거나 `FileSystemAccessRoleArn`을 사용하여 IAM 역할을 지정하는 경우 이 파라미터를 `TLS1_2`로 설정해야 합니다.

타입: 문자열

유효 값: `NONE | TLS1_2`

필수 여부: 아니요

Subdirectory

Amazon EFS 파일 시스템에 대한 탑재 경로를 지정합니다. DataSync가 파일 시스템의 데이터를 읽거나 쓰는 위치입니다(소스 위치인지 대상 위치인지에 따라 다름).

기본적으로 DataSync는 루트 디렉터리(또는 사용자가 `AccessPointArn`을 사용하여 루트 디렉터리를 제공하는 경우 액세스 포인트)를 사용합니다. 전방향 슬래시(예: `/path/to/folder`)를 사용하여 하위 디렉터리를 포함할 수도 있습니다.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

필수 여부: 아니요

Tags

리소스에 추가하려는 태그를 나타내는 키-값 쌍을 지정합니다. 값은 빈 문자열일 수도 있습니다. 이 값은 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 대한 이름 태그를 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

사용자가 생성하는 Amazon EFS 파일 시스템 위치의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

다음 예제에서는 Amazon EFS 파일 시스템에 대해 위치를 생성합니다.

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

샘플 요청: 제한된 Amazon EFS 파일 시스템에 대해 위치 생성

다음 예제에서는 액세스가 제한된 Amazon EFS 파일 시스템에 대해 위치를 생성합니다. 이런 종류의 시나리오에서는 요청에 `AccessPointArn`, `FileSystemAccessRoleArn`, 및 `InTransitEncryption`값을 지정해야 할 수 있습니다.

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

샘플 응답

응답은 Amazon EFS 파일 시스템의 위치 ARN을 반환합니다.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-12abcdef012345678"
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationFsxLustre

Amazon FSx for Lustre 파일 시스템의 전송 위치를 생성합니다.이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다.

시작하려면 먼저 DataSync에서 FSx for Lustre 파일 시스템에 액세스하는 방법을 이해해야 합니다.

구문 요청

```
{
   "FsxFilesystemArn": "string",
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

FsxFilesystemArn

FSx for Lustre 파일 시스템의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

필수 여부: 예

SecurityGroupArns

FSx for Lustre 파일 시스템에 대한 액세스 권한을 제공하는 최대 5개 보안 그룹의 Amazon 리소스 이름(ARN)을 지정합니다.

보안 그룹은 파일 시스템의 포트에 액세스할 수 있어야 합니다. 또한 파일 시스템은 보안 그룹의 액세스를 허용해야 합니다. 파일 시스템 액세스에 대한 자세한 내용은 Amazon FSx for Lustre 사용 설명서를 참조하세요.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

필수 여부: 예

Subdirectory

FSx for Lustre 파일 시스템에 대한 탑재 경로를 지정합니다. 경로에는 하위 디렉터리가 포함될 수 있습니다.

위치가 소스로 사용되는 경우 DataSync는 마운트 경로에서 데이터를 읽습니다. 위치가 대상으로 사용되는 경우 DataSync는 데이터를 탑재 경로에 기록합니다. 이 파라미터를 포함하지 않으면 DataSync는 파일 시스템의 루트 디렉터리(/)를 사용합니다.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 위치에 대한 이름 태그를 하나 이상 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

생성한 FSx for Lustre 파일 시스템 위치의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationFsxOntap

Amazon FSx for NetApp ONTAP 파일 시스템의 전송 위치를 생성합니다.이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다.

시작하려면 먼저 DataSync에서 FSx for ONTAP 파일 시스템에 액세스하는 방법을 이해해야 합니다.

구문 요청

```
{
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "CmkSecretConfig": {
            "KmsKeyArn": "string",
            "SecretArn": "string"
         },
         "CustomSecretConfig": {
            "SecretAccessRoleArn": "string",
            "SecretArn": "string"
         },
         "Domain": "string",
         "ManagedSecretConfig": {
            "SecretArn": "string"
         },
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "SecurityGroupArns": [ "string" ],
   "StorageVirtualMachineArn": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
```

```
        }
    ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Protocol

가 Amazon FSx 파일 시스템에 액세스하는 데 AWS DataSync 사용하는 데이터 전송 프로토콜을 지정합니다.

타입: FsxProtocol객체

필수 여부: 예

SecurityGroupArns

파일 시스템의 선호 서브넷에 대한 액세스를 제공하는 Amazon EC2 보안 그룹을 지정합니다.

보안 그룹은 (사용 중인 프로토콜에 따라) 다음 포트에서 아웃바운드 트래픽을 허용해야 합니다:

- NFS(Network File System): TCP 포트 111, 635 및 2,049
- SMB(Server Message Block): TCP 포트 445

파일 시스템의 보안 그룹은 동일한 포트에서 인바운드 트래픽도 허용해야 합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

필수 여부: 예

StorageVirtualMachineArn

데이터를 복사하려는 파일 시스템에서 스토리지 가상 머신(SVM)의 ARN을 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 162입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

필수 여부: 예

Subdirectory

데이터를 주고 받을 SVM에 파일 공유 경로를 지정합니다.

정션 경로(탑재 지점이라고도 함), qtree 경로(NFS 파일 공유의 경우) 또는 공유 이름(SMB 파일 공유의 경우)을 지정할 수 있습니다. 예를 들어, 탑재 경로는 `/vol1`, `/vol1/tree1`또는 `/share1`일 수 있습니다.

> **Note**
>
> SVM의 루트 볼륨에 정션 경로를 지정하지 않습니다. 자세한 설명은 Amazon FSx for NetApp ONTAP User Guide(Amazon FSx for NetApp ONTAP 사용자 가이드)의 Managing FSx for ONTAP storage virtual machines(FSx for ONTAP 스토리지 가상 머신 관리)를 참조하세요.

타입: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

필수 여부: 아니요

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 위치에 대한 이름 태그를 하나 이상 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

생성한 FSx for ONTAP 파일 시스템 위치에 대해 ARN을 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationFsxOpenZfs

Amazon FSx for OpenZFS 파일 시스템의 전송 위치를 생성합니다.이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다.

시작하려면 먼저 DataSync에서 FSx for OpenZFS 파일 시스템에 액세스하는 방법을 이해해야 합니다.

> **Note**
>
> SMB와 관련된 요청 파라미터는 `CreateLocationFsxOpenZfs`작업에서 지원되지 않습니다.

구문 요청

```
{
   "FsxFilesystemArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "CmkSecretConfig": {
            "KmsKeyArn": "string",
            "SecretArn": "string"
         },
         "CustomSecretConfig": {
            "SecretAccessRoleArn": "string",
            "SecretArn": "string"
         },
         "Domain": "string",
         "ManagedSecretConfig": {
            "SecretArn": "string"
         },
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
```

```
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

FsxFilesystemArn

FSx for OpenZFS 파일 시스템의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

필수 여부: 예

Protocol

가 파일 시스템에 액세스하는 데 AWS DataSync 사용하는 프로토콜 유형입니다.

타입: FsxProtocol객체

필수 여부: 예

SecurityGroupArns

FSx for OpenZFS 파일 시스템을 구성하는 데 사용되는 보안 그룹의 ARN입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

필수 여부: 예

Subdirectory

`/fsx`로 시작해야 하는 위치 경로의 하위 디렉터리입니다. DataSync는 이 하위 디렉터리를 사용하여 데이터를 읽거나 씁니다(파일 시스템이 소스 위치인지 목적지 위치인지에 따라 다름).

타입: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[^\u0000\u0085\u2028\u2029\r\n]{1,4096}$`

필수 여부: 아니요

Tags

리소스에 추가하려는 태그를 나타내는 키-값 쌍입니다. 값은 빈 문자열일 수도 있습니다. 이 값은 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 대한 이름 태그를 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

생성한 FSx for OpenZFS 파일 시스템 위치를 위한 FSx의 ARN.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationFsxWindows

Amazon FSx for Windows File Server 파일 시스템의 전송 위치를 생성합니다.이 위치를 데이터 전송의 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다.

시작하려면 먼저 DataSync에서 FSx for Windows File Server 파일 시스템에 액세스하는 방법을 이해해야 합니다.

구문 요청

```
{
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "Domain": "string",
   "FsxFilesystemArn": "string",
   "Password": "string",
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "User": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

CmkSecretConfig

DataSync가 고객 관리형 보안 암호에 대한 구성 정보를 지정합니다. 여기에는 DataSync가 고객 관리형 보안 암호로 특정 FSx Windows 스토리지 위치에 액세스하는 데 사용하는 암호가 포함됩니다 AWS KMS key.

이 파라미터를 `CreateLocationFsxWindows` 요청의 일부로 포함하는 경우 KMS 키 ARN만 제공합니다. DataSync는 `Password`에 대해 지정한와 함께이 KMS 키를 사용하여 위치 액세스 자격 증명을 저장하는 DataSync 관리형 보안 암호를 생성합니다.

DataSync에 지정한 KMS 키에 액세스할 수 있는 권한이 있는지 확인합니다. 자세한 내용은 사용자 지정으로 암호화된 서비스 관리형 보안 암호 사용을 참조하세요 AWS KMS key.

> **Note**
>
> `CmkSecretConfig`(`Password` 포함) 또는 `CustomSecretConfig`(`Password` 제외)을 사용하여 `CreateLocationFsxWindows` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

FSx for Windows File Server 스토리지 위치의 암호가 Secrets Manager에 일반 텍스트로 저장되는 고객 관리형 Secrets Manager 보안 암호의 구성 정보를 지정합니다. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다. 자세한 내용은 관리하는 보안 암호 사용을 참조하세요.

> **Note**
>
> `CmkSecretConfig`(`Password` 포함) 또는 `CustomSecretConfig`(`Password` 제외)을 사용하여 `CreateLocationFsxWindows` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CustomSecretConfig객체

필수 여부: 아니요

Domain

FSx for Windows File Server 파일 시스템이 속한 Windows 도메인의 이름을 지정합니다.

환경에 여러 Active Directory 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 파일 시스템에 연결되게 할 수 있습니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

필수 여부: 아니요

FsxFilesystemArn

FSx for Windows File Server 파일 시스템의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

필수 여부: 예

Password

FSx for Windows File Server 파일 시스템의 파일, 폴더, 파일 메타데이터를 탑재하고 이에 액세스할 수 있는 권한이 있는 사용자의 암호를 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^.{0,104}$`

필수 여부: 아니요

SecurityGroupArns

파일 시스템의 기본 설정 서브넷에 대한 액세스를 제공하는 Amazon EC2 보안 그룹의 ARN을 지정합니다.

지정한 보안 그룹은 파일 시스템의 보안 그룹과 통신할 수 있어야 합니다. 파일 시스템 액세스를 위한 보안 그룹 구성에 대한 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서를 참조하세요.

> **Note**
>
> 보안 그룹 자체 내 내부 연결을 허용하지 않는 보안 그룹을 선택한 경우 다음 중 하나를 수행합니다.
>
> - 보안 그룹 자체 내 통신을 허용하도록 보안 그룹 구성을 구성합니다.
> - 탑재 대상의 보안 그룹과 통신할 수 있는 다른 보안 그룹을 선택합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

필수 여부: 예

Subdirectory

슬래시를 사용하여 파일 시스템에 대한 탑재 경로를 지정합니다. DataSync가 데이터를 읽거나 쓰는 위치입니다(소스 위치인지 대상 위치인지에 따라 다름).

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 위치에 대한 이름 태그를 하나 이상 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

User

FSx for Windows File Server 파일 시스템의 파일, 폴더, 파일 메타베이터를 탑재하고 이에 액세스할 수 있는 권한이 있는 사용자를 지정합니다.

전송에 적합한 수준의 액세스 권한을 가진 사용자를 선택하는 방법에 대한 자세한 내용은 FSx for Windows File Server 위치에 필요한 권한을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

필수 여부: 예

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

생성한 FSx for Windows File Server 파일 시스템의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationHdfs

하둡 분산 파일 시스템(HDFS)의 전송 위치를 생성합니다.는이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다.

시작하기 전에 먼저 DataSync가 HDFS 클러스터에 액세스하는 방법을 이해해야 합니다.

구문 요청

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlockSize": number,
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "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"
      }
```

```
    ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArns

HDFS 클러스터에 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 예

AuthenticationType

사용자 ID를 결정하는 데 사용되는 인증 타입.

타입: 문자열

유효 값: `SIMPLE | KERBEROS`

필수 사항 여부: 예

BlockSize

HDFS 클러스터에 쓸 데이터 블록의 크기입니다. 블록 크기는 512바이트의 배수여야 합니다. 기본 블록 크기는 128메비바이트(MiB)입니다.

유형: 정수

유효한 범위: 최소값은 1048576입니다. 최대값은 1073741824입니다.

필수 여부: 아니요

CmkSecretConfig

DataSync가 고객 관리형으로 특정 Hadoop 분산 파일 시스템(HDFS) 스토리지 위치에 액세스하는 데 사용하는 Kerberos 키탭을 포함하는 DataSync 관리형 보안 암호의 구성 정보를 지정합니다 AWS KMS key.

이 파라미터를 `CreateLocationHdfs` 요청의 일부로 포함하는 경우 KMS 키 ARN만 제공합니다. DataSync는 `KerberosKeytab`에 대해 지정한와 함께이 KMS 키를 사용하여 위치 액세스 자격 증명을 저장하는 DataSync 관리형 보안 암호를 생성합니다.

DataSync에 지정한 KMS 키에 액세스할 수 있는 권한이 있는지 확인합니다. 자세한 내용은 사용자 지정으로 암호화된 서비스 관리형 보안 암호 사용을 참조하세요 AWS KMS key.

> **Note**
>
> `CmkSecretConfig(KerberosKeytab 포함)` 또는 `CustomSecretConfig(KerberosKeytab 제외)`을 사용하여 `CreateLocationHdfs` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

HDFS 스토리지 위치의 Kerberos 키 탭이 Secrets Manager의 이진수에 저장되는 고객 관리형 Secrets Manager 보안 암호에 대한 구성 정보를 지정합니다. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다. 자세한 내용은 관리하는 보안 암호 사용을 참조하세요.

> **Note**
>
> `CmkSecretConfig(KerberosKeytab 포함)` 또는 `CustomSecretConfig(KerberosKeytab 제외)`을 사용하여 `CreateLocationHdfs` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CustomSecretConfig객체

필수 여부: 아니요

KerberosKeytab

정의된 Kerberos 보안 주체와 암호화된 키 간의 매핑이 포함된 Kerberos 키 테이블(keytab)입니다. 파일 주소를 제공하여 파일에서 키탭을 로드할 수 있습니다.

> **Note**
>
> `AuthenticationType`에 `KERBEROS`가 지정된 경우 이 파라미터가 필요합니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 65536입니다.

필수 여부: 아니요

KerberosKrb5Conf

Kerberos 구성 정보가 포함된 `krb5.conf` 파일입니다. 파일 주소를 제공하여 `krb5.conf`파일을 로드할 수 있습니다. AWS CLI를 사용하는 경우, base64 인코딩을 자동으로 수행합니다. 그렇지 않으면 base64 인코딩 형식의 텍스트를 제공하십시오.

> **Note**
>
> `AuthenticationType`에 `KERBEROS`가 지정된 경우 이 파라미터가 필요합니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 131072입니다.

필수 여부: 아니요

KerberosPrincipal

HDFS 클러스터의 파일 및 폴더에 대한 액세스 권한이 있는 Kerberos 보안 주체입니다.

> **Note**
>
> `AuthenticationType`에 `KERBEROS`가 지정된 경우 이 파라미터가 필요합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^.+$`

필수 여부: 아니요

KmsKeyProviderUri

HDFS 클러스터의 키 관리 서버(KMS)의 URI입니다.

타입: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 255.

패턴: `^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$`

필수 여부: 아니요

NameNodes

HDFS 네임스페이스를 관리하는 NameNode입니다. NameNode는 파일 및 디렉터리 열기, 닫기 및 이름 바꾸기와 같은 작업을 수행합니다. NameNode에는 데이터 블록을 DataNode에 매핑하기 위한 정보가 들어 있습니다. 하나의 NameNode만 사용할 수 있습니다.

타입: HdfsNameNode객체 배열

어레이 멤버: 최소 항목 수 1개.

필수 항목 여부: 예

QopConfiguration

QOP(Quality of Protection) 구성은 Hadoop 분산 파일 시스템(HDFS) 클러스터에 구성된 원격 프로시저 호출(RPC) 및 데이터 전송 방지 설정을 지정합니다. `QopConfiguration`이 지정되지 않은 경우 `RpcProtection` 및 `DataTransferProtection`은 기본적으로 `PRIVACY`로 설정됩니다. `RpcProtection` 또는 `DataTransferProtection`을 설정하면 다른 파라미터는 동일한 값을 가정합니다.

유형: QopConfiguration객체

필수 여부: 아니요

ReplicationFactor

HDFS 클러스터에 쓸 때 데이터를 복제할 DataNode의 수입니다. 기본적으로 데이터는 3개의 DataNode에 복제됩니다.

타입: 정수

유효 범위: 최소값 1. 최대값은 512입니다.

필수 여부: 아니요

SimpleUser

호스트 운영 체제에서 클라이언트를 식별하는 데 사용되는 사용자 이름입니다.

> **Note**
>
> `AuthenticationType`에 `SIMPLE`가 지정된 경우 이 파라미터가 필요합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

필수 여부: 아니요

Subdirectory

HDFS 클러스터의 하위 디렉터리입니다. 이 하위 디렉터리는 HDFS 클러스터에서 데이터를 읽거나 쓰는 데 사용됩니다. 하위 디렉터리를 지정하지 않으면 기본적으로 `/`로 설정됩니다.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

Tags

위치에 추가하려는 태그를 나타내는 키-값 쌍입니다. 값은 빈 문자열일 수도 있습니다. 태그를 사용하여 리소스의 이름을 지정하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

생성하는 소스 HDFS 클러스터 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationNfs

NFS(Network File System) 파일 서버의 전송 위치를 생성합니다.이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다.

시작하기 전에 먼저 DataSync가 NFS 파일 서버에 액세스하는 방법을 이해해야 합니다.

구문 요청

```
{
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
   },
   "ServerHostname": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

MountOptions

DataSync가 NFS 파일 서버를 탑재하는 데 사용할 수 있는 옵션을 지정합니다.

유형: NfsMountOptions객체

필수 여부: 아니요

OnPremConfig

NFS 파일 서버에 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)을 지정합니다.

하나 이상의 에이전트를 지정할 수 있습니다. 자세한 내용은 Using multiple DataSync agents 섹션을 참조하세요.

타입: OnPremConfig객체

필수 항목 여부: 예

ServerHostname

DataSync 에이전트가 연결될 NFS 파일 서버의 DNS 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

필수 여부: 예

Subdirectory

DataSync에서 탑재할 NFS 파일 서버의 내보내기 경로를 지정합니다.

이 경로(또는 경로의 하위 디렉터리)는 DataSync가 데이터를 전송하고 전송 받는 곳입니다. DataSync용 내보내기 구성에 대한 자세한 내용은 NFS 파일 서버 액세스를 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]+$`

필수 여부: 예

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 위치에 이름 태그를 하나 이상 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

NFS 파일 서버용으로 생성한 전송 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예제

다음 예제에서는 NFS 파일 서버에 대한 DataSync 전송 위치를 생성합니다.

샘플 요청

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

예제

응답은 NFS 위치의 ARN을 반환합니다.

샘플 응답

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2

- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationObjectStorage

객체 스토리지 시스템의 전송 위치를 생성합니다.이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다. DataSync 에이전트를 사용하거나 사용하지 않고 전송할 수 있습니다.

시작하기 전에 DataSync가 객체 스토리지 시스템과 함께 작동하기 위한 사전 조건을 이해해야 합니다.

구문 요청

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

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccessKey

객체 스토리지 서버에 인증하는 데 자격 증명이 필요한 경우, 액세스 키(예: 사용자 이름)를 지정합니다.

유형: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: `^.*$`

필수 여부: 아니요

AgentArns

(선택 사항) 객체 스토리지 시스템과 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)을 지정합니다. 에이전트 없는 클라우드 간 전송을 설정하는 경우 이 파라미터에 값을 지정할 필요가 없습니다.

> **Note**
>
> 스토리지 위치를 처음 생성할 때 이 파라미터를 올바르게 구성해야 합니다. 에이전트를 생성한 후에는 스토리지 위치에서 에이전트를 추가하거나 제거할 수 없습니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

BucketName

전송과 관련된 객체 스토리지 버킷의 이름을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 63입니다.

패턴: ^[a-zA-Z0-9_\-\+\.\(\)\$\p{Zs}]+$

필수 여부: 예

CmkSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 지정합니다. 이는 DataSync가 고객 관리형 AWS KMS key와 함께 특정 객체 스토리지 위치에 액세스하는 데 사용하는 SecretKey를 포함합니다.

이 파라미터를 CreateLocationObjectStorage 요청의 일부로 포함하는 경우 KMS 키 ARN만 제공합니다. DataSync는이 KMS 키를 SecretKey 파라미터에 지정한 값과 함께 사용하여 DataSync 관리형 보안 암호를 생성하고 위치 액세스 자격 증명을 저장합니다.

DataSync에 지정한 KMS 키에 액세스할 수 있는 권한이 있는지 확인합니다. 자세한 내용은 사용자 지정으로 암호화된 서비스 관리형 보안 암호 사용을 참조하세요 AWS KMS key.

> **Note**
>
> CmkSecretConfig(SecretKey 포함) 또는 CustomSecretConfig(SecretKey 제외)을 사용하여 CreateLocationObjectStorage 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

특정 객체 스토리지 위치의 보안 키가 Secrets Manager에 일반 텍스트로 저장되는 고객 관리형 Secrets Manager 보안 암호의 구성 정보를 지정합니다. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다. 자세한 내용은 관리하는 보안 암호 사용을 참조하세요.

> **Note**
>
> CmkSecretConfig(SecretKey 포함) 또는 CustomSecretConfig(SecretKey 제외)을 사용하여 CreateLocationObjectStorage 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CustomSecretConfig객체

필수 여부: 아니요

SecretKey

객체 스토리지 서버에 인증하는 데 자격 증명이 필요한 경우, 보안 암호 키(예: 암호)를 지정합니다.

> **Note**
>
> 를 사용하여 보안 암호를 제공SecretKey하지만 CmkSecretConfig 또는를 사용하여 보안 암호 구성 세부 정보를 제공하지 않는 경우 CustomSecretConfig DataSync는 AWS 계정의 Secrets Manager 보안 암호를 사용하여 토큰을 저장합니다.

유형: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: `^.*$`

필수 여부: 아니요

ServerCertificate

시스템이 프라이빗 또는 자체 서명 인증 기관(CA)을 사용하는 경우 DataSync가 객체 스토리지 시스템으로 인증하기 위한 인증서 체인을 지정합니다. 전체 인증서 체인(예: `file:///home/user/.ssh/object_storage_certificates.pem`)이 있는 단일 `.pem` 파일을 지정해야 합니다.

인증서 체인에는 다음이 포함될 수 있습니다.

- 객체 스토리지 시스템의 인증서
- 모든 중간 인증서(있는 경우)
- 서명 CA의 루트 인증서

인증서를 `.pem` 파일로 연결할 수 있습니다(base64 인코딩 전 최대 32,768바이트). 다음 예제의 `cat` 명령은 세 개의 인증서가 포함된 `object_storage_certificates.pem` 파일을 생성합니다.

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

이 파라미터를 사용하려면 ServerProtocol를 HTTPS로 구성하세요.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 32768입니다.

필수 여부: 아니요

ServerHostname

DataSync 에이전트가 연결될 객체 스토리지 서버의 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

필수 여부: 예

ServerPort

객체 스토리지 서버가 인바운드 네트워크 트래픽을 수락하는 포트(예: 포트 443)를 지정합니다.

타입: 정수

유효 범위: 최소값 1. 최대값은 65536입니다.

필수 여부: 아니요

ServerProtocol

객체 스토리지 서버의 통신에 사용되는 프로토콜을 지정합니다. 지정하지 않은 경우 기본값은 HTTPS입니다.

타입: 문자열

유효 값: `HTTPS | HTTP`

필수 여부: 아니요

Subdirectory

객체 스토리지 서버의 객체 접두사를 지정합니다. 소스 위치인 경우, DataSync는 이 접두사가 있는 객체만 복사합니다. 목적지 위치인 경우, DataSync는 이 접두사가 있는 모든 객체를 씁니다.

타입: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

필수 여부: 아니요

Tags

리소스에 추가하려는 태그를 나타내는 키-값 쌍을 지정합니다. 태그는 리소스 관리, 필터링 및 검색에 도움이 됩니다. 위치에 이름 태그를 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

생성한 오브젝트 스토리지 시스템 위치의 ARN을 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationS3

Amazon S3 버킷의 전송 위치를 생성합니다. AWS DataSync 는 이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 수 있습니다.

> **Important**
>
> 시작하기 전에 다음 주제를 읽어보시기 바랍니다.
>
> - Amazon S3 위치의 스토리지 클래스 고려 사항
> - DataSync 사용 시 S3 요청 비용 평가

자세한 내용은 Configuring transfers with Amazon S3 섹션을 참조하세요.

구문 요청

```
{
   "AgentArns": [ "string" ],
   "S3BucketArn": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
   "S3StorageClass": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArns

(Amazon S3 on Outposts만 해당) Outpost에 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)을 지정합니다.

자세한 내용은 DataSync 에이전트 배포를 참조하세요 AWS Outposts.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

S3BucketArn

위치로 사용할 S3 버킷의 ARN을 지정합니다. (나중에 DataSync 작업을 생성할 때 이 위치가 전송 소스인지 대상인지를 지정합니다.)

S3 버킷이 AWS Outposts 리소스에 있는 경우 Amazon S3 액세스 포인트를 지정해야 합니다. 자세한 내용은 Amazon S3 사용 설명서에서 Amazon S3 액세스 포인트를 사용한 데이터 액세스 관리를 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 268입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

필수 여부: 예

S3Config

DataSync가 S3 버킷에 액세스하는 데 사용하는 (IAM) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (ARN)을 지정합니다.

자세한 내용은 DataSync에 S3 버킷 액세스 권한 제공을 참조하세요.

타입: S3Config객체

필수 항목 여부: 예

S3StorageClass

Amazon S3가 전송 대상일 때 객체가 사용할 스토리지 클래스를 지정합니다.

의 버킷 AWS 리전의 경우 스토리지 클래스의 기본값은 입니다STANDARD. 의 버킷 AWS Outposts 의 경우 스토리지 클래스의 기본값은 입니다OUTPOSTS.

자세한 내용은 Storage class considerations with Amazon S3 transfers 섹션을 참조하세요.

타입: 문자열

유효 값: `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

필수 여부: 아니요

Subdirectory

DataSync가 읽거나 쓰는 S3 버킷의 접두사를 입력합니다(버킷이 소스인지 대상 위치인지에 따라 다름).

> **Note**
>
> DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`
> - `photos/../2006/March`

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

필수 여부: 아니요

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 전송 위치에 대한 이름 태그를 적어도 하나 작성하는 것이 좋습니다.

유형: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

사용자가 생성한 S3 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateLocationSmb

SMB(Server Message Block) 파일 서버의 전송 위치를 생성합니다.이 위치를 데이터 전송을 위한 소스 또는 대상으로 사용할 AWS DataSync 수 있습니다.

시작하기 전에 먼저 DataSync가 SMB 파일 서버에 액세스하는 방법을 이해해야 합니다. 자세한 내용은 DataSync에 SMB 파일 서버 액세스 권한 제공을 참조하세요.

구문 요청

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosKeytab": blob,
   "KerberosKrb5Conf": blob,
   "KerberosPrincipal": "string",
   "MountOptions": {
      "Version": "string"
   },
   "Password": "string",
   "ServerHostname": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "User": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArns

SMB 파일 서버에 연결할 수 있는 DataSync 에이전트(또는 에이전트들)를 지정합니다. 에이전트의 Amazon 리소스 이름(ARN)을 사용하여 에이전트를 지정합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 예

AuthenticationType

DataSync가 SMB 파일 서버에 연결하는 데 사용하는 인증 프로토콜을 지정합니다. DataSync는 `NTLM`(기본값) 및 `KERBEROS` 인증을 지원합니다.

자세한 내용은 DataSync에 SMB 파일 서버 액세스 권한 제공을 참조하세요.

타입: 문자열

유효 값: `NTLM | KERBEROS`

필수 여부: 아니요

CmkSecretConfig

DataSync가 고객 관리형를 사용하여 특정 SMB 스토리지 위치에 액세스하는 데 사용하는 `Password` 또는 `KerberosKeytab` (각각 `NTLM` (기본값) 및 `KERBEROS` 인증 유형) 중 하나인 DataSync 관리형 보안 암호에 대한 구성 정보를 지정합니다 AWS KMS key.

이 파라미터를 `CreateLocationSmbRequest` 요청의 일부로 포함하는 경우 KMS 키 ARN만 제공합니다. DataSync는이 KMS 키를 `Password` 또는 `KerberosKeytab` 사용자가 지정한와 함께 사용하여 DataSync 관리형 보안 암호를 생성하여 위치 액세스 자격 증명을 저장합니다.

DataSync에 지정한 KMS 키에 액세스할 수 있는 권한이 있는지 확인합니다. 자세한 내용은 사용자 지정으로 암호화된 서비스 관리형 보안 암호 사용을 참조하세요 AWS KMS key.

> **Note**
>
> CmkSecretConfig (Password 또는와 함께KerberosKeytab) 또는 CustomSecretConfig (Password 및 없이KerberosKeytab)를 사용하여 CreateLocationSmbRequest 요청에 대한 자격 증명을 제공할 수 있습니다. 동일한 요청에 대해 CmkSecretConfig 및 CustomSecretConfig 파라미터를 모두 제공하지 마십시오.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

SMB 스토리지 위치 보안 인증 정보가 Secrets Manager에 일반 텍스트(용) 또는 바이너리(용Password)로 저장되는 고객 관리형 Secrets Manager 보안 암호의 구성 정보를 지정합니다KerberosKeytab. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다. 자세한 내용은 관리하는 보안 암호 사용을 참조하세요.

> **Note**
>
> CmkSecretConfig(SasConfiguration 포함) 또는 CustomSecretConfig(SasConfiguration 제외)을 사용하여 CreateLocationSmbRequest 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CustomSecretConfig객체

필수 여부: 아니요

DnsIpAddresses

SMB 파일 서버가 속한 DNS 서버의 IPv4 또는 IPv6 주소를 지정합니다. 이 파라미터는 AuthenticationType이 KERBEROS로 설정된 경우에만 적용됩니다.

환경에 여러 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 SMB 파일 서버에 연결되도록 할 수 있습니다.

유형: 문자열 배열

배열 멤버: 최대 항목 수는 2개입니다.

길이 제약: 최소 길이는 7입니다. 최대 길이는 39입니다.

패턴: `\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`

필수 여부: 아니요

Domain

SMB 파일 서버가 속한 Windows 도메인 이름을 지정합니다. 이 파라미터는 `AuthenticationType`이 `NTLM`로 설정된 경우에만 적용됩니다.

환경에 여러 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 파일 서버에 연결되도록 할 수 있습니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

필수 여부: 아니요

KerberosKeytab

Kerberos 보안 주체와 암호화 키 간의 매핑을 포함하는 Kerberos 키 테이블(keytab) 파일을 지정합니다.

작업 실행 오류를 방지하려면 키탭 파일을 생성하는 데 사용하는 Kerberos 보안 주체가 `KerberosPrincipal`에 지정한 것과 정확히 일치하는지 확인합니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 65536입니다.

필수 여부: 아니요

KerberosKrb5Conf

Kerberos 영역 구성을 정의하는 Kerberos 구성 파일(krb5.conf)을 지정합니다.

파일은 반드시 base64로 인코딩되어야 합니다. 를 사용하는 경우 AWS CLI인코딩이 수행됩니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 131072입니다.

필수 여부: 아니요

KerberosPrincipal

Kerberos 영역에서 SMB 파일 서버의 파일, 폴더, 파일 메타데이터에 액세스할 수 있는 권한을 가진 Kerberos 보안 주체를 지정합니다.

Kerberos 보안 주체는 HOST/kerberosuser@MYDOMAIN.ORG처럼 보일 수 있습니다.

보안 주체 이름은 대/소문자를 구분합니다. 이 파라미터에 대해 지정한 보안 주체가 키탭 파일 생성에 사용하는 보안 주체와 정확히 일치하지 않으면 DataSync 작업 실행이 실패합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: ^.+$

필수 여부: 아니요

MountOptions

DataSync가 SMB 파일 서버에 액세스하는 데 사용하는 SMB 프로토콜의 버전을 지정합니다.

타입: SmbMountOptions객체

필수 여부: 아니요

Password

사용자 SMB 파일 서버를 탑재하고 전송과 관련된 파일과 폴더에 액세스할 수 있는 권한이 있는 사용자의 암호를 지정합니다. 이 파라미터는 AuthenticationType이 NTLM로 설정된 경우에만 적용됩니다.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^.{0,104}$`

필수 여부: 아니요

ServerHostname

DataSync 에이전트가 연결될 SMB 파일 서버의 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다.

> **Note**
>
> Kerberos 인증을 사용하는 경우 도메인 이름을 지정해야 합니다.

유형: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

필수 여부: 예

Subdirectory

DataSync가 데이터를 읽거나 쓸 SMB 파일 서버에서 내보낸 공유의 이름을 지정합니다. 공유 경로에 하위 디렉토리(예: `/path/to/subdirectory`)를 포함할 수 있습니다. 네트워크의 다른 SMB 클라이언트도 이 경로를 마운트할 수 있는지 확인하세요.

하위 디렉터리의 모든 데이터를 복사하려면 DataSync가 SMB 공유를 마운트하고 모든 데이터에 액세스할 수 있어야 합니다. 자세한 내용은 DataSync에 SMB 파일 서버 액세스 권한 제공을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 예

Tags

AWS 리소스를 분류, 필터링 및 검색하는 데 도움이 되는 레이블을 지정합니다. 위치에 대한 이름 태그를 하나 이상 생성하는 것이 좋습니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

User

SMB 파일 서버의 파일, 폴더, 파일 메타데이터를 탑재하고 액세스할 수 있는 사용자를 지정합니다. 이 파라미터는 `AuthenticationType`이 `NTLM`로 설정된 경우에만 적용됩니다.

전송에 적합한 수준의 액세스 권한을 가진 사용자를 선택하는 방법에 대한 자세한 내용은 SMB 파일 서버에 대한 DataSync 액세스 제공을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

필수 여부: 아니요

응답 구문

```
{
   "LocationArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

LocationArn

귀하가 생성한 SMB 위치의 ARN입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

다음 예에서는 SMB 파일 서버의 위치를 생성합니다.

```
{
   "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"
}
```

샘플 응답

응답은 SMB 파일 서버의 위치 ARN을 반환합니다.

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

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

CreateTask

AWS DataSync 가 데이터를 이동하는 위치와 방법을 정의하는 작업을 구성합니다.

작업에는 소스 위치, 대상 위치, 전송 옵션(예: 대역폭 제한, 예약 등)이 포함됩니다.

> **Important**
>
> Amazon S3 위치와 데이터를 주고받을 계획이라면 시작하기 전에 DataSync가 S3 요청 요금에 미치는 영향 및 DataSync 요금 페이지를 검토하세요.

구문 요청

```
{
   "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"
   }
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

CloudWatchLogGroupArn

작업을 모니터링하기 위한 Amazon CloudWatch 로그 그룹의 Amazon 리소스 이름(ARN)을 지정합니다.

확장 모드 작업의 경우 아무것도 지정할 필요가 없습니다. DataSync는 `/aws/datasync`라는 CloudWatch 로그 그룹에 로그를 자동으로 전송합니다.

자세한 내용은 CloudWatch Logs를 사용하여 데이터 전송 모니터링을 참조하세요.

유형: 문자열

길이 제약 조건: 최대 길이는 562입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

필수 여부: 아니요

DestinationLocationArn

전송 대상 위치의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

Excludes

DataSync가 전송하지 않도록 소스 위치의 파일, 객체 및 폴더를 정의하는 제외 필터를 지정합니다. 자세한 내용과 예제는 Specifying what DataSync transfers by using filters 섹션을 참조하세요.

타입: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

Includes

DataSync로 전송하려는 소스 위치의 파일, 객체, 폴더를 정의하는 포함 필터를 지정합니다. 자세한 내용과 예제는 Specifying what DataSync transfers by using filters 섹션을 참조하세요.

타입: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

ManifestConfig

DataSync에서 전송하려는 파일 또는 객체 목록인 매니페스트를 구성합니다. 자세한 내용과 구성 예제는 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

이 파라미터를 사용할 때는 발신자 자격 증명(DataSync를 사용하는 역할)에 `iam:PassRole` 권한이 있어야 합니다. AWSDataSyncFullAccess 정책에는 이 권한이 포함됩니다.

유형: ManifestConfig객체

필수 여부: 아니요

Name

작업의 이름을 지정합니다.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

Options

파일 메타데이터 보존, 데이터 무결성 확인 등의 작업 설정을 지정합니다.

유형: Options객체

필수 여부: 아니요

Schedule

작업을 실행할 일정을 지정합니다. 자세한 내용을 알아보려면 태스크 예약을 참조하십시오.

유형: TaskSchedule객체

필수 여부: 아니요

SourceLocationArn

전송 소스 위치의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

Tags

작업에 적용할 태그를 지정합니다.

태그는 DataSync 리소스를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다.

유형: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

TaskMode

데이터 전송을 위해 다음 작업 모드 중 하나를 지정합니다.

- ENHANCED - 기본 모드보다 성능이 뛰어난 객체를 사실상 무제한으로 전송합니다. 확장 모드 작업은 데이터를 병렬로 나열, 준비, 전송, 확인하여 데이터 전송 프로세스를 최적화합니다. 확장 모드는 현재 Amazon S3 위치 간 전송, 에이전트 없이 Azure Blob과 Amazon S3 간 전송, 에이전트 없이 다른 클라우드와 Amazon S3 간 전송에 사용할 수 있습니다.

  > **Note**
  >
  > 확장 모드 작업을 생성하려면 `CreateTask` 작업을 호출하는 데 사용하는 IAM 역할에 `iam:CreateServiceLinkedRole` 권한이 있어야 합니다.

- BASIC(기본값) - AWS 스토리지와 지원되는 다른 모든 DataSync 위치 간에 파일 또는 객체를 전송합니다. 기본 모드 작업에는 데이터세트의 파일, 객체, 디렉터리 수에 대한 할당량이 적용됩니다. 기본 모드는 데이터를 순차적으로 준비, 전송, 확인하므로 대부분의 워크로드에서 확장 모드보다 느립니다.

자세한 내용은 작업 모드 차이점 이해를 참조하세요.

타입: 문자열

유효 값: `BASIC | ENHANCED`

필수 여부: 아니요

TaskReportConfig

DataSync 전송에 대한 세부 정보를 제공하는 작업 보고서를 구성할 방법을 지정합니다. 자세한 내용은 Monitoring your DataSync transfers with task reports 섹션을 참조하세요.

이 파라미터를 사용할 때는 발신자 자격 증명(DataSync를 사용하는 역할)에 `iam:PassRole` 권한이 있어야 합니다. AWSDataSyncFullAccess 정책에는 이 권한이 포함됩니다.

유형: TaskReportConfig객체

필수 항목 여부: 아니요

응답 구문

```
{
```

```
   "TaskArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

TaskArn

작업의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

확장 모드 작업에 대한 샘플 요청

다음 예시에서는 확장 모드를 사용하는 DataSync 작업을 생성합니다.

기본 모드 작업을 생성할 때와 달리 Amazon CloudWatch 로그 그룹을 지정할 필요가 없습니다. 확장 모드 작업에서 DataSync는 작업 로그를 /aws/datasync라는 이름의 로그 그룹으로 자동 전송합니다. 해당 로그 그룹이에 없는 경우 AWS 리전 DataSync는 작업을 생성할 때 사용자를 대신하여 로그 그룹을 생성합니다.

```
{
  "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"
  }
}
```

기본 모드 작업에 대한 샘플 요청

다음 예시에서는 기본 모드를 사용하는 DataSync 작업을 생성합니다.

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

샘플 응답

다음 응답은 생성된 작업의 ARN을 포함합니다.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DeleteAgent

에서 AWS DataSync 에이전트 리소스를 제거합니다 AWS 계정.

이 작업(취소할 수 없음)은 에이전트의 가상 머신 또는 Amazon EC2 인스턴스를 스토리지 환경에서 제거하지 않는다는 점에 유의하세요. 다음 단계에서는 스토리지 환경에서 VM 또는 인스턴스를 삭제하거나 이를 새 에이전트 활성화에 재 사용할 수 있습니다.

구문 요청

```
{
   "AgentArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArn

삭제할 에이전트의 Amazon 리소스 이름(ARN)입니다. `ListAgents` 작업을 사용하여 계정 및의 에이전트 목록을 반환합니다 AWS 리전.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 예

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DeleteLocation

전송 위치 리소스를 삭제합니다 AWS DataSync.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

삭제할 위치의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DeleteTask

전송 작업 리소스를 삭제합니다 AWS DataSync.

구문 요청

```
{
   "TaskArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

TaskArn

삭제하려는 작업의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

필수 여부: 예

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeAgent

이름, 서비스 엔드포인트 유형 및 상태와 같은 AWS DataSync 에이전트에 대한 정보를 반환합니다.

구문 요청

```
{
   "AgentArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArn

정보를 원하는 DataSync 에이전트의 Amazon 리소스 이름(ARN) 을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "AgentArn": "string",
   "CreationTime": number,
   "EndpointType": "string",
   "LastConnectionTime": number,
   "Name": "string",
   "Platform": {
      "Version": "string"
   },
   "PrivateLinkConfig": {
```

```
      "PrivateLinkEndpoint": "string",
      "SecurityGroupArns": [ "string" ],
      "SubnetArns": [ "string" ],
      "VpcEndpointId": "string"
   },
   "Status": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AgentArn

에이전트의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

에이전트가 활성화된 시간.

유형: 타임스탬프

EndpointType

사용자 에이전트가 연결된 서비스 엔드포인트의 유형입니다.

타입: 문자열

유효 값: `PUBLIC | PRIVATE_LINK | FIPS | FIPS_PRIVATE_LINK`

LastConnectionTime

에이전트가 DataSync 서비스와 마지막으로 통신한 시간입니다.

유형: 타임스탬프

Name

에이전트의 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

Platform

에이전트에 대한 플랫폼 관련 세부 정보(예: 버전 번호)

유형: Platform객체

PrivateLinkConfig

에이전트가 VPC 서비스 엔드포인트에 연결할 때 사용하는 네트워크 구성입니다.

유형: PrivateLinkConfig객체

Status

에이전트의 상태.

- 상태가 `ONLINE`이면 에이전트가 제대로 구성되어 사용할 준비가 된 것입니다.
- 상태가 `OFFLINE`이면 에이전트가 5분 이상 동안 DataSync와 연락이 끊긴 것입니다. 몇 가지 원인이 있을 수 있습니다. 자세한 내용은 에이전트가 오프라인 상태인 경우 어떻게 하나요? 를 확인하세요.

타입: 문자열

유효 값: `ONLINE | OFFLINE`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

다음 예는 요청에 지정된 에이전트에 대한 정보를 반환합니다.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0"
}
```

샘플 응답

다음 예제 응답은 공용 서비스 엔드포인트를 사용하는 에이전트를 설명합니다.

```
{
    "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"
    }
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++

- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationAzureBlob

Microsoft Azure Blob Storage의 AWS DataSync 전송 위치가 구성되는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

Azure Blob 스토리지 전송 위치의 Amazon 리소스 이름(ARN) 을 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "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"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AccessTier

객체 또는 파일을 전송하려는 액세스 티어. 이는 해당 위치를 전송 대상으로 사용하는 경우에만 적용됩니다. 자세한 내용은 액세스 티어를 참조하세요.

타입: 문자열

유효 값: `HOT | COOL | ARCHIVE`

AgentArns

Azure Blob 스토리지 컨테이너와 연결할 수 있는 DataSync 에이전트의 ARN

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

DataSync가 Azure Blob 스토리지에 액세스하는 데 사용하는 인증 방법입니다. DataSync는 공유 액세스 서명(SAS)을 사용하여 블롭 스토리지에 액세스할 수 있습니다.

타입: 문자열

유효 값: `SAS | NONE`

BlobType

개체 또는 파일을 Azure Blob Storage로 전송할 때 사용하려는 블럽 타입입니다. 현재 DataSync는 데이터를 블록으로 Azure Blob Storage로 이동하는 것만 지원합니다. 블롭 유형에 대한 자세한 내용은 Azure Blob Storage 설명서를 참조하세요.

타입: 문자열

유효 값: `BLOCK`

CmkSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 설명하며, 여기에는 DataSync가 고객 관리형 AWS KMS key와 함께 특정 스토리지 위치에 액세스하는 데 사용하는 인증 토큰이 포함됩니다.

유형: CmkSecretConfig객체

CreationTime

Azure Blob Storage 전송 위치가 생성된 시간입니다.

유형: 타임스탬프

CustomSecretConfig

DataSync가 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할을 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 인증 토큰과 같은 고객 관리형 보안 암호의 구성 정보를 설명합니다.

유형: CustomSecretConfig객체

LocationArn

Azure 블럽 스토리지 전송 위치의 ARN입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

전송과 관련된 Azure Blob 스토리지 컨테이너의 URL.

타입: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 설명하며, 여기에는 DataSync가 특정 스토리지 위치에 액세스하는 데 사용하는 인증 토큰이 포함됩니다. DataSync는 기본 AWS관리형 KMS 키를 사용하여이 보안 암호를 암호화합니다 AWS Secrets Manager.

타입: ManagedSecretConfig 객체

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++

- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationEfs

Amazon EFS 파일 시스템의 AWS DataSync 전송 위치를 구성하는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

정보를 확인하려는 Amazon EFS 파일 시스템 위치의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "AccessPointArn": "string",
   "CreationTime": number,
   "Ec2Config": {
      "SecurityGroupArns": [ "string" ],
      "SubnetArn": "string"
   },
   "FileSystemAccessRoleArn": "string",
   "InTransitEncryption": "string",
```

```
    "LocationArn": "string",
    "LocationUri": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AccessPointArn

DataSync가 Amazon EFS 파일 시스템에 액세스하는 데 사용하는 액세스 지점의 ARN입니다.

자세한 내용은 Accessing restricted file systems 섹션을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

CreationTime

위치가 생성된 시간.

유형: 타임스탬프

Ec2Config

가 Amazon EFS 파일 시스템의 탑재 대상 중 하나에 연결하는 데 AWS DataSync 사용하는 서브넷 및 보안 그룹입니다.

유형: Ec2Config객체

FileSystemAccessRoleArn

DataSync가 Amazon EFS 파일 시스템에 액세스할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할입니다.

자세한 내용은 Creating a DataSync IAM role for file system access 섹션을 참조하세요.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

InTransitEncryption

DataSync가 Amazon EFS 파일 시스템으로 또는 파일 시스템에서 데이터를 전송할 때 Transport Layer Security(TLS) 암호화를 사용하는지 여부를 나타냅니다.

타입: 문자열

유효 값: `NONE | TLS1_2`

LocationArn

Amazon EFS 파일 시스템 위치의 ARN입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

Amazon EFS 파일 시스템 위치의 URL입니다.

타입: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

다음의 예는 특정 Amazon EFS 파일 시스템 위치에 대한 정보를 가져오는 방법을 알려줍니다.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-12abcdef012345678"
}
```

샘플 응답

다음 예에서는 Amazon EFS 파일 시스템의 위치 세부 정보를 반환합니다.

```
{
    "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/"
}
```

샘플 응답: 제한된 Amazon EFS 파일 시스템의 위치 설명

다음 예는 `AccessPointArn`, `FileSystemAccessRoleArn`, `InTransitEncryption`요소를 포함하여 액세스가 제한된 Amazon EFS 파일 시스템에 대한 위치 세부 정보를 반환합니다.

```
{
```

```
    "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"
    }]
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationFsxLustre

Amazon FSx for Lustre 파일 시스템의 AWS DataSync 전송 위치가 구성되는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

설명할 FSx for Lustre 위치의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "SecurityGroupArns": [ "string" ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

FSx for Lustre 위치가 생성된 시간입니다.

타입: Timestamp

LocationArn

FSx for Lustre 위치의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

FSx for Lustre 위치의 URI입니다.

타입: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

FSx for Lustre 파일 시스템에 대해 구성된 보안 그룹의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationFsxOntap

Amazon FSx for NetApp ONTAP 파일 시스템의 AWS DataSync 전송 위치가 구성되는 방법에 대한 세부 정보를 제공합니다.

> **Note**
>
> 위치에서 SMB를 사용하는 경우 `DescribeLocationFsxOntap`작업은 실제로 `Password`를 반환하지 않습니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

정보를 확인하려는 FSx for ONTAP 파일 시스템 위치의 Amazon 리소스 이름(ARN)을 명시합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "CreationTime": number,
```

```
   "FsxFilesystemArn": "string",
   "LocationArn": "string",
   "LocationUri": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "CmkSecretConfig": {
            "KmsKeyArn": "string",
            "SecretArn": "string"
         },
         "CustomSecretConfig": {
            "SecretAccessRoleArn": "string",
            "SecretArn": "string"
         },
         "Domain": "string",
         "ManagedSecretConfig": {
            "SecretArn": "string"
         },
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "SecurityGroupArns": [ "string" ],
   "StorageVirtualMachineArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

위치가 생성된 시간.

유형: 타임스탬프

FsxFilesystemArn

FSx for ONTAP 파일 시스템의 ARN.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:file-system/fs-[0-9a-f]+$`

LocationArn

FSx for ONTAP 파일 시스템 위치의 ARN.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

FSx for ONTAP 파일 시스템 위치의 URI(균일 리소스 식별자).

유형: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

가 Amazon FSx 파일 시스템에 액세스하는 데 AWS DataSync 사용하는 데이터 전송 프로토콜을 지정합니다.

유형: FsxProtocol객체

SecurityGroupArns

DataSync가 FSx for ONTAP 파일 시스템에 액세스하는 데 사용하는 보안 그룹.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

StorageVirtualMachineArn

데이터를 복사할 FSx for ONTAP 파일 시스템의 스토리지 가상 머신(SVM)의 ARN.

유형: 문자열

길이 제약: 최대 길이는 162입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++

- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationFsxOpenZfs

Amazon FSx for OpenZFS 파일 시스템의 AWS DataSync 전송 위치가 구성되는 방법에 대한 세부 정보를 제공합니다.

> **Note**
>
> SMB와 관련된 응답 요소는 `DescribeLocationFsxOpenZfs`작업에서 지원되지 않습니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

설명할 FSx for OpenZFS 위치의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
```

```
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "CmkSecretConfig": {
            "KmsKeyArn": "string",
            "SecretArn": "string"
         },
         "CustomSecretConfig": {
            "SecretAccessRoleArn": "string",
            "SecretArn": "string"
         },
         "Domain": "string",
         "ManagedSecretConfig": {
            "SecretArn": "string"
         },
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "SecurityGroupArns": [ "string" ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

FSx for OpenZFS 위치가 생성된 시간입니다.

유형: 타임스탬프

LocationArn

FSx for OpenZFS 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

FSx for OpenZFS 위치의 통합 리소스 식별자(URI)입니다.

예시: `fsxz://us-west-2.fs-1234567890abcdef02/fsx/folderA/folder`

유형: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

가 파일 시스템에 액세스하는 데 AWS DataSync 사용하는 프로토콜 유형입니다.

유형: FsxProtocol객체

SecurityGroupArns

FSx for OpenZFS 파일 시스템을 구성하는 보안 그룹의 ARN입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationFsxWindows

Amazon FSx for Windows File Server 파일 시스템의 AWS DataSync 전송 위치를 구성하는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

FSx for Windows File Server 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CreationTime": number,
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
```

```
   },
   "Domain": "string",
   "LocationArn": "string",
   "LocationUri": "string",
   "ManagedSecretConfig": {
      "SecretArn": "string"
   },
   "SecurityGroupArns": [ "string" ],
   "User": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CmkSecretConfig

DataSync가 고객 관리형를 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 등 `Password` DataSync 관리형 보안 암호의 구성 정보를 설명합니다 AWS KMS key.

유형: CmkSecretConfig객체

CreationTime

FSx for Windows File Server가 생성된 시간입니다.

유형: 타임스탬프

CustomSecretConfig

`Password` DataSync가 보안 암호에 대한 액세스를 제공하는 고객 관리형(IAM) 역할을 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 등 고객 관리형 AWS Identity and Access Management 보안 암호에 대한 구성 정보를 설명합니다.

유형: CustomSecretConfig객체

Domain

FSx for Windows File Server 파일 시스템이 속한 Microsoft Active Directory 도메인의 이름입니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

LocationArn

FSx for Windows File Server 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

FSx for Windows File Server 위치의 Uniform Resource Identifier(URI)입니다.

유형: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

DataSync가 특정 스토리지 위치에 액세스하는 데 사용하는와 같은 `Password` DataSync 관리형 보안 암호의 구성 정보를 설명합니다. DataSync는 기본 AWS관리형 KMS 키를 사용하여이 보안 암호를 암호화합니다 AWS Secrets Manager.

유형: ManagedSecretConfig객체

SecurityGroupArns

파일 시스템의 기본 설정 서브넷에 대한 액세스를 제공하는 Amazon EC2 보안 그룹의 ARN입니다.

파일 시스템 액세스를 위한 보안 그룹 구성에 대한 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서를 참조하세요.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

User

FSx for Windows File Server 파일 시스템을 마운트하고 액세스할 수 있는 권한이 있는 사용자입니다.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationHdfs

하둡 분산 파일 시스템(HDFS)의 AWS DataSync 전송 위치가 구성되는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

HDFS 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlockSize": number,
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CreationTime": number,
```

```
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "KerberosPrincipal": "string",
   "KmsKeyProviderUri": "string",
   "LocationArn": "string",
   "LocationUri": "string",
   "ManagedSecretConfig": {
      "SecretArn": "string"
   },
   "NameNodes": [
      {
         "Hostname": "string",
         "Port": number
      }
   ],
   "QopConfiguration": {
      "DataTransferProtection": "string",
      "RpcProtection": "string"
   },
   "ReplicationFactor": number,
   "SimpleUser": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AgentArns

HDFS 클러스터와 연결할 수 있는 DataSync 에이전트의 ARN입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

사용자 ID를 결정하는 데 사용되는 인증 타입.

타입: 문자열

유효 값: `SIMPLE | KERBEROS`

BlockSize

HDFS 클러스터에 쓸 데이터 블록의 크기.

타입: 정수

유효한 범위: 최소값은 1048576입니다. 최대값은 1073741824입니다.

CmkSecretConfig

DataSync가 고객 관리형를 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 등 `KerberosKeytab` DataSync 관리형 보안 암호의 구성 정보를 설명합니다 AWS KMS key.

유형: CmkSecretConfig객체

CreationTime

HDFS 위치가 생성된 시간입니다.

유형: 타임스탬프

CustomSecretConfig

`KerberosKeytab` DataSync가 보안 암호에 대한 액세스를 제공하는 고객 관리형(IAM) 역할을 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 등 고객 관리형 AWS Identity and Access Management 보안 암호에 대한 구성 정보를 설명합니다.

유형: CustomSecretConfig객체

KerberosPrincipal

HDFS 클러스터의 파일 및 폴더에 대한 액세스 권한이 있는 Kerberos 보안 주체입니다. 이 파라미터는(`AuthenticationType`이)가(`KERBEROS`으)로 정의된 경우에 사용됩니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: ^.+$

KmsKeyProviderUri

HDFS 클러스터의 키 관리 서버(KMS)의 URI입니다.

타입: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 255.

패턴: ^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

HDFS 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: ^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$

LocationUri

HDFS 위치의 URI입니다.

유형: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: ^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$

ManagedSecretConfig

DataSync가 특정 스토리지 위치에 액세스하는 데 사용하는와 같은 KerberosKeytab DataSync 관리형 보안 암호의 구성 정보를 설명합니다. DataSync는 기본 AWS관리형 KMS 키를 사용하여이 보안 암호를 암호화합니다 AWS Secrets Manager.

유형: ManagedSecretConfig객체

NameNodes

HDFS 네임스페이스를 관리하는 NameNode입니다.

타입: HdfsNameNode객체 배열

어레이 멤버: 최소 항목 수 1개.

QopConfiguration

Quality of Protection(QOP) 구성은 HDFS 클러스터에 구성된 Remote Procedure Call(RPC) 및 데이터 전송 방지 설정을 지정합니다.

유형: QopConfiguration객체

ReplicationFactor

HDFS 클러스터에 쓸 때 데이터를 복제할 DataNode의 수입니다.

타입: 정수

유효 범위: 최소값 1. 최대값은 512입니다.

SimpleUser

호스트 운영 체제에서 클라이언트를 식별하는 사용자 이름입니다. 이 파라미터는 (`AuthenticationType`이)가(`SIMPLE`으)로 정의된 경우에 사용됩니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationNfs

NFS(Network File System) 파일 서버의 AWS DataSync 전송 위치가 구성되는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

정보를 원하는 NFS 위치의 Amazon 리소스 이름 (ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
```

```
    }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CreationTime

NFS 위치가 생성된 시간입니다.

유형: 타임스탬프

LocationArn

NFS 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

NFS 위치의 URI입니다.

유형: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

MountOptions

DataSync가 사용자 NFS 파일 서버를 탑재하는 데 사용하는 탑재 옵션입니다.

유형: NfsMountOptions객체

OnPremConfig

NFS(Network File System) 파일 서버에 연결할 수 있는 AWS DataSync 에이전트입니다.

타입: OnPremConfig 객체

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예제

다음 예는 샘플 요청에 지정된 NFS 위치에 대한 정보를 반환합니다.

샘플 요청

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

예제

이 예제에서는 DescribeLocationNFS의 한 가지 사용법을 보여줍니다.

샘플 응답

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

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationObjectStorage

객체 스토리지 시스템의 AWS DataSync 전송 위치를 구성하는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

객체 스토리지 시스템 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "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"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AccessKey

객체 스토리지 시스템 인증에 필요한 액세스 키(예: 사용자 이름).

유형: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: `^.*$`

AgentArns

객체 스토리지 시스템과 연결할 수 있는 DataSync 에이전트의 ARN입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CmkSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 설명하며, 여기에는 DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트와 고객 관리형 AWS KMS key가 포함됩니다.

유형: CmkSecretConfig객체

CreationTime

위치가 생성된 시간.

유형: 타임스탬프

CustomSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트, 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할과 같은 고객 관리형 보안 암호의 구성 정보를 설명합니다.

유형: CustomSecretConfig객체

LocationArn

오브젝트 스토리지 시스템 위치의 ARN.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

객체 스토리지 시스템 위치의 URI입니다.

유형: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 설명하며, 여기에는 DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트가 포함됩니다. DataSync는 기본 AWS관리형 KMS 키를 사용하여이 보안 암호를 암호화합니다 AWS Secrets Manager.

유형: ManagedSecretConfig객체

ServerCertificate

시스템이 프라이빗 또는 자체 서명 인증 기관(CA)을 사용하는 경우 DataSync가 객체 스토리지 시스템으로 인증하기 위한 인증서 체인입니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약 조건: 최대 길이는 32768입니다.

ServerPort

객체 스토리지 서버가 인바운드 네트워크 트래픽을 수락하는 포트 (예: 포트 443).

타입: 정수

유효 범위: 최소값 1. 최댓값은 65536입니다.

ServerProtocol

객체 스토리지 시스템이 통신에 사용하는 프로토콜.

타입: 문자열

유효 값: `HTTPS | HTTP`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeLocationS3

S3 버킷의 AWS DataSync 전송 위치가 구성되는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

Amazon S3 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "AgentArns": [ "string" ],
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
   "S3StorageClass": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AgentArns

Amazon S3 on Outposts 작업을 사용할 때 Outpost에 배포된 DataSync 에이전트의 ARN입니다.

자세한 내용은 DataSync 에이전트 배포를 참조하세요 AWS Outposts.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

Amazon S3 위치가 생성된 시간입니다.

유형: 타임스탬프

LocationArn

Amazon S3 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

설명된 Amazon S3 위치의 URL입니다.

타입: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

S3Config

DataSync가 S3 버킷에 액세스하는 데 사용하는 (IAM) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (ARN)을 지정합니다.

자세한 내용은 DataSync에 S3 버킷 액세스 권한 제공을 참조하세요.

유형: S3Config객체

S3StorageClass

Amazon S3가 대상 위치인 경우 객체에 대해 선택한 스토리지 클래스입니다.

일부 스토리지 클래스에는 Amazon S3 스토리지 비용에 영향을 미칠 수 있는 동작이 있습니다. 자세한 내용은 Storage class considerations with Amazon S3 transfers 섹션을 참조하세요.

타입: 문자열

유효 값: `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예제

다음 예제는 샘플 요청에 지정된 Amazon S3 위치에 대한 정보를 반환합니다.

샘플 요청

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

예제

이 예에서는 DescribeLocations3의 한 가지 사용법을 보여줍니다.

샘플 응답

```
{
   "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"
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS SDK for Ruby V3

DescribeLocationSmb

SMB(Server Message Block) 파일 서버의 AWS DataSync 전송 위치를 구성하는 방법에 대한 세부 정보를 제공합니다.

구문 요청

```
{
   "LocationArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

정보를 원하는 SMB 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

응답 구문

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CreationTime": number,
   "CustomSecretConfig": {
```

```
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosPrincipal": "string",
   "LocationArn": "string",
   "LocationUri": "string",
   "ManagedSecretConfig": {
      "SecretArn": "string"
   },
   "MountOptions": {
      "Version": "string"
   },
   "User": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AgentArns

사용자의 SMB 파일 서버와 연결할 수 있는 DataSync 에이전트의 ARN입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

DataSync가 SMB 파일 서버에 연결하는 데 사용하는 인증 프로토콜입니다.

타입: 문자열

유효 값: `NTLM | KERBEROS`

CmkSecretConfig

DataSync가 고객 관리형를 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 Password 또는와 같은 KerberosKeytab DataSync 관리형 보안 암호의 구성 정보를 설명합니다 AWS KMS key.

유형: CmkSecretConfig객체

CreationTime

SMB 위치가 생성된 시간입니다.

유형: 타임스탬프

CustomSecretConfig

KerberosKeytab DataSync가 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할을 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 Password 또는와 같은 고객 관리형 보안 암호의 구성 정보를 설명합니다.

유형: CustomSecretConfig객체

DnsIpAddresses

SMB 파일 서버가 속한 DNS 서버의 IPv4 또는 IPv6 주소입니다. 이 값은 AuthenticationType이 KERBEROS로 설정된 경우에만 적용됩니다.

유형: 문자열 배열

배열 멤버: 최대 항목 수는 2개입니다.

길이 제약: 최소 길이는 7입니다. 최대 길이는 39입니다.

패턴: `\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

SMB 파일 서버가 속한 Windows 도메인의 이름입니다. 이 값은 AuthenticationType이 NTLM로 설정된 경우에만 적용됩니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

KerberosPrincipal

SMB 파일 서버의 파일, 폴더, 파일 메타데이터에 액세스할 권한이 있는 Kerberos 보안 주체입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^.+$`

LocationArn

SMB 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

SMB 위치의 URI입니다.

유형: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

DataSync가 특정 스토리지 위치에 액세스하는 데 사용하는 `Password` 또는와 같은 `KerberosKeytab` DataSync 관리형 보안 암호의 구성 정보를 설명합니다. DataSync는 기본 AWS 관리형 KMS 키를 사용하여이 보안 암호를 암호화합니다 AWS Secrets Manager.

유형: ManagedSecretConfig객체

MountOptions

DataSync가 SMB 파일 서버에 액세스하는 데 사용하는 SMB 프로토콜의 버전입니다.

유형: SmbMountOptions객체

User

SMB 파일 서버의 파일, 폴더, 파일 메타데이터를 탑재하고 액세스할 수 있는 사용자입니다. 이 값은 `AuthenticationType`이 `NTLM`로 설정된 경우에만 적용됩니다.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예제

이 예에서는 DescribeLocationSMB의 한 가지 사용법을 보여줍니다.

예 요청

```
{
```

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

예제

이 예에서는 DescribeLocationSMB의 한 가지 사용법을 보여줍니다.

샘플 응답

```
{
   "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"
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeTask

AWS DataSync 가 데이터를 전송하는 위치와 방법을 정의하는 작업에 대한 정보를 제공합니다.

구문 요청

```
{
   "TaskArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

TaskArn

정보를 원하는 전송의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

필수 여부: 예

응답 구문

```
{
   "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"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

CloudWatchLogGroupArn

작업을 모니터링하기 위한 Amazon CloudWatch 로그 그룹의 Amazon 리소스 이름(ARN)입니다.

자세한 내용은 CloudWatch Logs를 사용하여 데이터 전송 모니터링을 참조하세요.

유형: 문자열

길이 제약 조건: 최대 길이는 562입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

CreationTime

작업이 생성된 시각입니다.

유형: 타임스탬프

CurrentTaskExecutionArn

가장 최근 작업 실행의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

DestinationLocationArn

전송 대상 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

DestinationNetworkInterfaceArns

DataSync가 대상 위치에 생성한 네트워크 인터페이스의 ARN입니다.

유형: 문자열 배열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

ErrorCode

작업에 문제가 있는 경우 오류 코드를 사용하여 문제를 해결할 수 있습니다. 자세한 내용은 Troubleshooting issues with DataSync transfers 섹션을 참조하세요.

유형: 문자열

ErrorDetail

작업에 문제가 있는 경우 오류 세부 정보를 사용하여 문제를 해결할 수 있습니다. 자세한 내용은 Troubleshooting issues with DataSync transfers 섹션을 참조하세요.

유형: 문자열

Excludes

DataSync가 전송하지 않도록 소스 위치의 파일, 객체 및 폴더를 정의하는 제외 필터입니다. 자세한 내용과 예제는 Specifying what DataSync transfers by using filters 섹션을 참조하세요.

타입: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

Includes

DataSync가 전송할 소스 위치의 파일, 객체 및 폴더를 정의하는 포함 필터입니다. 자세한 내용과 예제는 Specifying what DataSync transfers by using filters 섹션을 참조하세요.

타입: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

ManifestConfig

DataSync가 전송할 파일 또는 객체를 나열하는 매니페스트의 구성입니다. 자세한 내용은 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

유형: ManifestConfig객체

Name

작업의 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

Options

작업의 설정입니다. 예를 들어 보존되는 파일 메타데이터, 전송 종료 시 데이터 무결성 확인 방법, 대역폭 제한 등 여러 옵션이 있습니다.

유형: Options객체

Schedule

작업을 실행할 일정입니다. 자세한 내용을 알아보려면 태스크 예약을 참조하십시오.

유형: TaskSchedule객체

ScheduleDetails

작업 일정에 대한 세부 정보입니다.

유형: TaskScheduleDetails객체

SourceLocationArn

전송 소스 위치의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

SourceNetworkInterfaceArns

DataSync가 소스 위치에 생성한 네트워크 인터페이스의 ARN입니다.

유형: 문자열 배열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

Status

작업의 상태입니다. 각 상태의 의미에 대한 자세한 내용은 Task statuses 섹션을 참조하세요.

타입: 문자열

유효 값: `AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE`

TaskArn

작업의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

TaskMode

사용 중인 작업 모드입니다. 자세한 내용은 데이터 전송을 위한 작업 모드 선택을 참조하세요.

타입: 문자열

유효 값: `BASIC | ENHANCED`

TaskReportConfig

DataSync 전송에 대한 세부 정보를 제공하는 작업 보고서 구성입니다. 자세한 내용은 Monitoring your DataSync transfers with task reports 섹션을 참조하세요.

타입: TaskReportConfig 객체

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

다음 예시에서는 정보를 가져올 DataSync 작업의 ARN을 지정합니다.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

샘플 응답

다음 예시에서는 DescribeTask 응답을 보여 줍니다.

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

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DescribeTaskExecution

AWS DataSync 작업 실행에 대한 정보를 제공합니다. 이 작업을 사용하면 진행 중인 데이터 전송 상황을 모니터링하거나 전송 결과를 확인할 수 있습니다.

> **Note**
>
> 일부 DescribeTaskExecution 응답 요소는 특정 작업 모드에만 적용됩니다. 자세한 내용은 작업 모드 차이 이해 및 데이터 전송 성능 카운터 이해를 참조하세요.

구문 요청

```
{
   "TaskExecutionArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

TaskExecutionArn

정보를 원하는 작업 진행의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

필수 여부: 예

응답 구문

```
{
   "BytesCompressed": number,
   "BytesTransferred": number,
```

```
   "BytesWritten": number,
   "EndTime": number,
   "EstimatedBytesToTransfer": number,
   "EstimatedFilesToDelete": number,
   "EstimatedFilesToTransfer": number,
   "EstimatedFoldersToDelete": number,
   "EstimatedFoldersToTransfer": number,
   "Excludes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "FilesDeleted": number,
   "FilesFailed": {
      "Delete": number,
      "Prepare": number,
      "Transfer": number,
      "Verify": number
   },
   "FilesListed": {
      "AtDestinationForDelete": number,
      "AtSource": number
   },
   "FilesPrepared": number,
   "FilesSkipped": number,
   "FilesTransferred": number,
   "FilesVerified": number,
   "FoldersDeleted": number,
   "FoldersFailed": {
      "Delete": number,
      "List": number,
      "Prepare": number,
      "Transfer": number,
      "Verify": number
   },
   "FoldersListed": {
      "AtDestinationForDelete": number,
      "AtSource": number
   },
   "FoldersPrepared": number,
   "FoldersSkipped": number,
   "FoldersTransferred": number,
   "FoldersVerified": number,
```

```
   "Includes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "LaunchTime": number,
   "ManifestConfig": {
      "Action": "string",
      "Format": "string",
      "Source": {
         "S3": {
            "BucketAccessRoleArn": "string",
            "ManifestObjectPath": "string",
            "ManifestObjectVersionId": "string",
            "S3BucketArn": "string"
         }
      }
   },
   "Options": {
      "Atime": "string",
      "BytesPerSecond": number,
      "Gid": "string",
      "LogLevel": "string",
      "Mtime": "string",
      "ObjectTags": "string",
      "OverwriteMode": "string",
      "PosixPermissions": "string",
      "PreserveDeletedFiles": "string",
      "PreserveDevices": "string",
      "SecurityDescriptorCopyFlags": "string",
      "TaskQueueing": "string",
      "TransferMode": "string",
      "Uid": "string",
      "VerifyMode": "string"
   },
   "ReportResult": {
      "ErrorCode": "string",
      "ErrorDetail": "string",
      "Status": "string"
   },
   "Result": {
      "ErrorCode": "string",
      "ErrorDetail": "string",
```

```
      "PrepareDuration": number,
      "PrepareStatus": "string",
      "TotalDuration": number,
      "TransferDuration": number,
      "TransferStatus": "string",
      "VerifyDuration": number,
      "VerifyStatus": "string"
   },
   "StartTime": number,
   "Status": "string",
   "TaskExecutionArn": "string",
   "TaskMode": "string",
   "TaskReportConfig": {
      "Destination": {
         "S3": {
            "BucketAccessRoleArn": "string",
            "S3BucketArn": "string",
            "Subdirectory": "string"
         }
      },
      "ObjectVersionIds": "string",
      "OutputType": "string",
      "Overrides": {
         "Deleted": {
            "ReportLevel": "string"
         },
         "Skipped": {
            "ReportLevel": "string"
         },
         "Transferred": {
            "ReportLevel": "string"
         },
         "Verified": {
            "ReportLevel": "string"
         }
      },
      "ReportLevel": "string"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

BytesCompressed

DataSync가 압축(가능한 경우) 후 네트워크를 통해 전송하는 물리적 바이트 수입니다. 일반적으로 이 수치는 데이터를 압축할 수 없는 경우를 제외하고 BytesTransferred보다 작습니다.

타입: Long

BytesTransferred

DataSync가 압축(가능한 경우) 전에 네트워크에 전송하는 바이트 수입니다. 네트워크를 통해 전송된 바이트 수는 BytesCompressed 섹션을 참조하세요.

타입: Long

BytesWritten

DataSync가 실제로 대상 위치에 기록한 논리적 바이트 수입니다.

타입: Long

EndTime

전송 작업이 종료되는 시간입니다.

유형: 타임스탬프

EstimatedBytesToTransfer

DataSync가 대상 위치에 기록할 것으로 예상되는 논리적 바이트 수입니다.

타입: Long

EstimatedFilesToDelete

DataSync가 대상 위치에서 삭제할 것으로 예상되는 파일, 객체, 디렉터리 수입니다. 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성하지 않는 경우 값은 항상 `0`입니다.

> **Note**
> 확장 모드 작업의 경우이 카운터에는 파일 또는 객체만 포함됩니다. 디렉터리는 EstimatedFoldersToDelete에 포함됩니다.

타입: Long

EstimatedFilesToTransfer

네트워크를 통해 DataSync가 전송할 것으로 예상되는 파일, 객체, 디렉터리 수입니다. 이 값은 DataSync가 전송을 준비하는 동안 계산됩니다.

계산 방법은 주로 작업의 전송 모드 구성에 따라 달라집니다.

- `TranserMode`이 `CHANGED`로 설정된 경우 - 계산은 소스와 대상의 위치 콘텐츠를 비교하고 이를 바탕으로 전송해야 하는 차이를 결정합니다. 차이점은 다음과 같습니다.
  - 소스 위치에 추가되거나 수정된 모든 항목입니다.
  - 두 위치 모두에 있고 초기 전송 후 대상에서 수정된 모든 항목(OverwriteMode가 `NEVER`로 설정된 경우 제외)입니다.
  - (기본 작업 모드 전용) DataSync가 삭제할 것으로 예상되는 항목의 수입니다 (PreserveDeletedFiles이 `REMOVE`로 설정된 경우).
- `TranserMode`가 `ALL`로 설정된 경우 - 계산은 DataSync가 소스 위치에서 찾는 항목만 기반으로 합니다.

> **Note**
>
> 확장 모드 작업의 경우이 카운터에는 파일 또는 객체만 포함됩니다. 디렉터리는 EstimatedFoldersToTransfer에 포함됩니다.

타입: Long

EstimatedFoldersToDelete

DataSync가 대상 위치에서 삭제할 것으로 예상되는 디렉터리 수입니다. 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성하지 않는 경우 값은 항상 `0`입니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

타입: Long

EstimatedFoldersToTransfer

DataSync가 네트워크를 통해 전송할 것으로 예상되는 디렉터리 수입니다. 이 값은 DataSync가 전송할 디렉터리를 준비할 때 계산됩니다.

계산 방법은 주로 작업의 전송 모드 구성에 따라 달라집니다.

- `TranserMode`이 `CHANGED`로 설정된 경우 - 계산은 소스와 대상의 위치 콘텐츠를 비교하고 이를 바탕으로 전송해야 하는 차이를 결정합니다. 차이점은 다음과 같습니다.
  - 소스 위치에 추가되거나 수정된 모든 항목입니다.
  - 두 위치 모두에 있고 초기 전송 후 대상에서 수정된 모든 항목(OverwriteMode가 `NEVER`로 설정된 경우 제외)입니다.
- `TranserMode`가 `ALL`로 설정된 경우 - 계산은 DataSync가 소스 위치에서 찾는 항목만 기반으로 합니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

타입: Long

Excludes

전송 중 특정 데이터를 제외하는 필터 규칙의 목록입니다. 자세한 내용과 예제는 DataSync에서 전송된 데이터 필터링을 참조하십시오.

유형: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

FilesDeleted

DataSync가 실제로 대상 위치에서 삭제한 파일, 객체, 디렉터리 수입니다. 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성하지 않는 경우 값은 항상 `0`입니다.

> **Note**
>
> 향상된 모드 작업의 경우이 카운터에는 파일 또는 객체만 포함됩니다. 디렉터리는 FoldersDeleted에 포함됩니다.

타입: Long

FilesFailed

DataSync가 작업 실행 중에 준비, 전송, 확인 및 삭제하지 못하는 파일 또는 객체의 수입니다.

> **Note**
> 확장 모드 작업에만 적용됩니다.

유형: TaskExecutionFilesFailedDetail객체

FilesListed

DataSync가 사용자 위치에서 찾는 파일 또는 객체의 수입니다.

> **Note**
> 확장 모드 작업에만 적용됩니다.

유형: TaskExecutionFilesListedDetail객체

FilesPrepared

소스 위치와 대상 위치를 비교한 후 DataSync가 전송을 시도할 파일 또는 객체의 수입니다.

> **Note**
> 확장 모드 작업에만 적용됩니다.

모든 데이터를 전송하도록 작업을 구성하는 경우 이 카운터를 사용할 수 없습니다. 이 시나리오에서 DataSync는 위치 간의 차이를 비교하지 않고 소스의 모든 데이터를 대상으로 복사합니다.

타입: Long

FilesSkipped

DataSync가 전송 중에 건너뛴 파일, 객체, 디렉터리의 수입니다.

> **Note**
> 확장 모드 작업의 경우이 카운터에는 파일 또는 객체만 포함됩니다. 디렉터리는 FoldersSkipped에 포함됩니다.

타입: Long

FilesTransferred

DataSync가 네트워크를 통해 실제로 전송한 파일, 객체, 디렉터리 수입니다. 이 값은 작업 실행 중 소스에서 무언가를 읽어 네트워크를 통해 전송할 때 주기적으로 업데이트됩니다.

DataSync가 무언가를 전송하지 못하면 이 값은 `EstimatedFilesToTransfer`보다 작을 수 있습니다. 경우에 따라 이 값은 `EstimatedFilesToTransfer`보다 클 수도 있습니다. 이 요소는 일부 위치 유형에서 구현 방식에 따라 달라지므로 이를 정확한 지표로서 사용하거나 작업 실행을 모니터링하는 데 사용하지 마세요.

> **Note**
>
> 확장 모드 작업의 경우이 카운터에는 파일 또는 객체만 포함됩니다. 디렉터리는 FoldersTransferred에 포함됩니다.

타입: Long

FilesVerified

DataSync가 전송 중에 확인한 파일, 객체, 디렉터리의 수입니다.

> **Note**
>
> 전송된 데이터만 확인하도록 작업을 구성하면 DataSync는 전송에 실패한 일부 상황이나 파일에서 디렉터리를 확인하지 않습니다.
> 향상된 모드 작업의 경우이 카운터에는 파일 또는 객체만 포함됩니다. 디렉터리는 FoldersVerified에 포함됩니다.

타입: Long

FoldersDeleted

DataSync가 대상 위치에서 실제로 삭제하는 디렉터리 수입니다. 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성하지 않는 경우 값은 항상 `0`입니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

타입: Long

FoldersFailed

DataSync가 작업 실행 중에 나열, 준비, 전송, 확인 및 삭제하지 못하는 디렉터리 수입니다.

> **Note**
> 확장 모드 작업에만 적용됩니다.

유형: TaskExecutionFoldersFailedDetail객체

FoldersListed

DataSync가 사용자 위치에서 찾는 디렉터리 수입니다.

> **Note**
> 확장 모드 작업에만 적용됩니다.

유형: TaskExecutionFoldersListedDetail객체

FoldersPrepared

소스 위치와 대상 위치를 비교한 후 DataSync가 전송을 시도할 디렉터리 수입니다.

> **Note**
> 확장 모드 작업에만 적용됩니다.

모든 데이터를 전송하도록 작업을 구성하는 경우 이 카운터를 사용할 수 없습니다. 이 시나리오에서 DataSync는 위치 간의 차이를 비교하지 않고 소스의 모든 데이터를 대상으로 복사합니다.

타입: Long

FoldersSkipped

전송 중에 DataSync가 건너뛰는 디렉터리 수입니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

타입: Long

FoldersTransferred

DataSync가 네트워크를 통해 실제로 전송하는 디렉터리 수입니다. 이 값은 작업 실행 중 소스에서 무언가를 읽어 네트워크를 통해 전송할 때 주기적으로 업데이트됩니다.

DataSync가 무언가를 전송하지 못하면 이 값은 `EstimatedFoldersToTransfer`보다 작을 수 있습니다. 경우에 따라 이 값은 `EstimatedFoldersToTransfer`보다 클 수도 있습니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

타입: Long

FoldersVerified

DataSync가 전송 중에 확인하는 디렉터리 수입니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

타입: Long

Includes

전송 중 특정 데이터를 포함하는 필터 규칙의 목록입니다. 자세한 내용과 예제는 DataSync에서 전송된 데이터 필터링을 참조하십시오.

유형: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

LaunchTime

작업 실행이 실제로 시작되는 시간입니다. 대기열에 추가되지 않은 작업의 경우 LaunchTime 및 StartTime은 일반적으로 같습니다. 대기 중인 작업의 경우, 일반적으로 먼저 대기 중인 작업의 실행이 완료된 후에 새 작업이 시작되므로 LaunchTime이 StartTime보다 늦습니다.

유형: 타임스탬프

ManifestConfig

전송할 파일 또는 객체를 나열하는 매니페스트의 구성입니다. 자세한 내용은 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

유형: ManifestConfig객체

Options

전송 작업이 구성된 방식을 나타냅니다. 이러한 옵션에는 DataSync가 전송 중에 파일, 객체 및 관련 메타데이터 처리 방법이 포함됩니다. 또한 다른 옵션 중에서 데이터 무결성을 확인하고, 작업에 대한 대역폭 제한 설정 방법을 지정할 수 있습니다.

각 옵션에는 기본값이 있습니다. 필요한 경우가 아니라면 StartTaskExecution을 호출하기 전에 이러한 옵션을 구성하지 않아도 됩니다.

각 작업 실행에 대해 작업 옵션을 재정의할 수도 있습니다. 예를 들어 개별 실행에 대해 LogLevel을 조정할 수 있습니다.

유형: Options객체

ReportResult

DataSync가 전송에 대한 전체 작업 보고서를 생성했는지 여부를 나타냅니다.

유형: ReportResult객체

Result

작업 실행 결과입니다.

유형: TaskExecutionResultDetail객체

StartTime

DataSync가 작업 실행을 시작하기 위해 요청을 전송하는 시간입니다. 대기열에 추가되지 않은 작업의 경우 LaunchTime 및 StartTime은 일반적으로 같습니다. 대기 중인 작업의 경우,

일반적으로 먼저 대기 중인 작업의 실행이 완료된 후에 새 작업이 시작되므로 LaunchTime이 StartTime보다 늦습니다.

유형: 타임스탬프

Status

작업 실행 상태입니다.

작업 실행 상태에 대한 자세한 내용은 작업 실행 상태를 참조하세요.

타입: 문자열

유효 값: QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR

TaskExecutionArn

정보를 원했던 작업 실행의 ARN입니다. TaskExecutionArn은 계층적이며 실행된 작업의 TaskArn를 포함합니다.

예를 들어, ARN arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2/execution/exec-08ef1e88ec491019b이 있는 TaskExecution값은 ARN으로 작업 arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2을 실행했습니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: ^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$

TaskMode

사용 중인 작업 모드입니다. 자세한 내용은 데이터 전송을 위한 작업 모드 선택을 참조하세요.

타입: 문자열

유효 값: BASIC | ENHANCED

TaskReportConfig

DataSync 전송에 대한 세부 정보를 제공하는 작업 보고서 구성입니다. 자세한 내용은 작업 보고서 생성을 참조하십시오.

타입: TaskReportConfig 객체

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

이 예제는 DescribeTaskExecution요청을 보여줍니다.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1"
}
```

확장 모드 작업 실행에 대한 샘플 응답 1

다음 예시에서는 확장 모드를 사용하는 DataSync 작업 실행을 설명합니다. 해당 실행은 또한 제외 및 포함 필터를 사용하여 특정 데이터를 전송합니다.

```
{
    "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,
    "EstimatedFoldersToTransfer": 2,
    "EstimatedBytesToTransfer": 30,
    "FilesTransferred": 7,
    "FoldersTransferred": 2,
    "BytesWritten": 30,
    "BytesTransferred": 30,
    "BytesCompressed": 30,
    "Result": {
        "PrepareDuration": 0,
        "PrepareStatus": "SUCCESS",
        "TotalDuration": 3310,
        "TransferDuration": 0,
        "TransferStatus": "SUCCESS",
        "VerifyDuration": 0,
        "VerifyStatus": "SUCCESS"
    },
    "FilesDeleted": 0,
    "FilesSkipped": 0,
    "FilesVerified": 7,
    "EstimatedFilesToDelete": 0,
    "TaskMode": "ENHANCED",
    "FilesPrepared": 7,
    "FilesListed": {
```

```
        "AtSource": 7,
        "AtDestinationForDelete": 0
    },
    "FilesFailed": {
        "Prepare": 0,
        "Transfer": 0,
        "Verify": 0,
        "Delete": 0
    },
    "FoldersDeleted": 0,
    "FoldersSkipped": 0,
    "FoldersVerified": 2,
    "FoldersPrepared": 2,
    "FoldersListed": {
        "AtSource": 2,
        "AtDestinationForDelete": 0
    },
    "FoldersFailed": {
        "List": 0,
        "Prepare": 0,
        "Transfer": 0,
        "Verify": 0,
        "Delete": 0
    }
}
```

확장 모드 작업 실행에 대한 샘플 응답 2

다음 예시에서는 확장 모드를 사용하는 또 다른 DataSync 작업 실행을 설명합니다. 이 경우 해당 실행은 필터 대신 매니페스트를 사용하여 특정 데이터를 전송합니다.

```
{
    "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,
    "EstimatedFoldersToTransfer": 0,
    "EstimatedBytesToTransfer": 6,
    "FilesTransferred": 1,
    "FoldersTransferred": 1,
    "BytesWritten": 6,
    "BytesTransferred": 6,
    "BytesCompressed": 6,
    "Result": {
        "PrepareDuration": 0,
        "PrepareStatus": "SUCCESS",
        "TotalDuration": 3089,
        "TransferDuration": 0,
        "TransferStatus": "SUCCESS",
        "VerifyDuration": 0,
```

```
        "VerifyStatus": "SUCCESS"
    },
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "Subdirectory": "reports/",
                "S3BucketArn": "arn:aws:s3:::my-task-report",
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-task-report-
role/DataSyncTaskReportS3BucketAccess"
            }
        },
        "OutputType": "STANDARD",
        "ReportLevel": "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
    },
    "FoldersDeleted": 0,
    "FoldersSkipped": 0,
    "FoldersVerified": 0,
    "FoldersPrepared": 0,
    "FoldersListed": {
        "AtSource": 0,
        "AtDestinationForDelete": 0
    },
    "FoldersFailed": {
        "List": 0,
```

```
        "Prepare": 0,
        "Transfer": 0,
        "Verify": 0,
        "Delete": 0
    }
  }
```

기본 모드 작업 실행에 대한 샘플 응답

다음 예시에서는 기본 모드를 사용하는 DataSync 작업 실행을 설명합니다.

```
{
    "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"
    }
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go v2용 SDK
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

ListAgents

요청에 AWS 리전 지정된의 AWS 계정 에 속하는 AWS DataSync 에이전트 목록을 반환합니다.

페이지 매김을 사용하면 응답에서 반환되는 상담원 수를 줄일 수 있습니다. 응답에서 상담원 목록이 잘린 경우, 응답에는 다음 상담원 페이지를 가져오도록 요청에서 지정할 수 있는 마커가 포함됩니다.

`ListAgents`은 결국 일관성을 갖습니다. 즉, 작업을 실행한 결과에 에이전트를 방금 만들거나 삭제했다는 사실이 반영되지 않을 수 있습니다. 예컨대, CreateAgent를 사용하여 에이전트를 만든 다음 즉시 `ListAgents`를 실행하면, 해당 에이전트가 목록에 바로 표시되지 않을 수 있습니다. 이와 같은 상황에서는 DescribeAgent를 사용하여 에이전트가 생성(또는 삭제) 되었는지 언제든지 확인할 수 있습니다.

구문 요청

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

MaxResults

응답에 표시할 수 있는 최대 DataSync 에이전트 수를 지정합니다. 기본적으로 응답에는 최대 100개의 에이전트가 표시됩니다.

타입: Integer

유효 범위: 최소값은 0입니다. 최댓값은 100입니다.

필수 여부: 아니요

NextToken

응답에서 다음 결과 목록의 시작 위치를 표시하는 불투명 문자열을 지정합니다.

타입: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: [a-zA-Z0-9=_-]+

필수 여부: 아니요

응답 구문

```
{
   "Agents": [
      {
         "AgentArn": "string",
         "Name": "string",
         "Platform": {
            "Version": "string"
         },
         "Status": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Agents

요청에 AWS 리전 지정된의 AWS 계정 에 있는 DataSync 에이전트 목록입니다. 목록은 에이전트의 Amazon 리소스 이름(ARN) 순으로 정렬됩니다.

타입: AgentListEntry객체 배열

NextToken

응답에서 다음 결과 목록을 시작할 위치를 표시하는 불투명한 문자열입니다.

타입: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: [a-zA-Z0-9=_-]+

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

ListLocations

소스 및 목적지 위치의 목록을 반환합니다.

응답에 반환된 위치보다 많은 위치가 있는 경우,(즉, 응답에서 상담원의 잘린 목록만 반환되는 경우) 응답에는 다음 위치 페이지를 가져오기 위한 요청에서 지정할 수 있는 토큰이 포함됩니다.

구문 요청

```
{
   "Filters": [
      {
         "Name": "string",
         "Operator": "string",
         "Values": [ "string" ]
      }
   ],
   "MaxResults": number,
   "NextToken": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Filters

API 필터를 사용하여 `ListLocations`에 의해 반환되는 리소스 목록의 범위를 좁힐 수 있습니다. 예컨대, 특정 소스 위치에서 모든 작업을 검색하려면 필터 이름 `LocationType S3`및 `Operator Equals`과 함께 `ListLocations`을 사용할 수 있습니다.

타입: LocationFilter객체 배열

필수 여부: 아니요

MaxResults

반환할 위치의 최대수.

타입: Integer

유효 범위: 최소값은 0입니다. 최댓값은 100입니다.

필수 여부: 아니요

NextToken

다음 위치 목록을 시작할 위치를 표시하는 불투명한 문자열입니다.

타입: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: `[a-zA-Z0-9=_-]+`

필수 여부: 아니요

응답 구문

```
{
   "Locations": [
      {
         "LocationArn": "string",
         "LocationUri": "string"
      }
   ],
   "NextToken": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Locations

위치 목록이 포함된 배열입니다.

타입: LocationListEntry객체 배열

NextToken

다음 위치 목록 반환을 시작할 위치를 표시하는 불투명 문자열입니다.

타입: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: `[a-zA-Z0-9=_-]+`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

ListTagsForResource

AWS 리소스와 연결된 모든 태그를 반환합니다.

구문 요청

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ResourceArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

MaxResults

귀하가 응답에서 몇 개의 결과를 원하는지를 지정합니다.

유형: 정수

유효 범위: 최소값은 0입니다. 최댓값은 100입니다.

필수 여부: 아니요

NextToken

응답에서 다음 결과 목록의 시작 위치를 표시하는 불투명 문자열을 지정합니다.

타입: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: `[a-zA-Z0-9=_-]+`

필수 여부: 아니요

ResourceArn

태그 정보를 사용하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(((agent|task|location)/(agent|task|loc)-[a-z0-9]{17}(/execution/exec-[a-f0-9]{17})?)|(system/storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}(/job/discovery-job-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})?))$`

필수 여부: 예

응답 구문

```
{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

응답에서 다음 결과 목록을 시작할 위치를 표시하는 불투명한 문자열입니다.

타입: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: `[a-zA-Z0-9=_-]+`

Tags

지정된 리소스에 적용되는 태그의 배열입니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 55개입니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

ListTaskExecutions

AWS DataSync 전송 작업에 대한 실행 목록을 반환합니다.

구문 요청

```
{
   "MaxResults": number,
   "NextToken": "string",
   "TaskArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

MaxResults

응답에서 원하는 결과 수를 지정합니다.

유형: 정수

유효 범위: 최소값은 0입니다. 최댓값은 100입니다.

필수 여부: 아니요

NextToken

응답에서 다음 결과 목록이 시작하는 위치를 표시하는 불투명 문자열을 지정합니다.

유형: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: `[a-zA-Z0-9=_-]+`

필수 여부: 아니요

TaskArn

실행 정보를 원하는 작업의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

필수 여부: 아니요

응답 구문

```
{
   "NextToken": "string",
   "TaskExecutions": [
      {
         "Status": "string",
         "TaskExecutionArn": "string",
         "TaskMode": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

응답에서 다음 결과 목록을 시작할 위치를 표시하는 불투명한 문자열입니다.

타입: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: `[a-zA-Z0-9=_-]+`

TaskExecutions

작업의 실행 목록입니다.

타입: TaskExecutionListEntry 객체 배열

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

ListTasks

생성한 AWS DataSync 작업 목록을 반환합니다.

구문 요청

```
{
   "Filters": [
      {
         "Name": "string",
         "Operator": "string",
         "Values": [ "string" ]
      }
   ],
   "MaxResults": number,
   "NextToken": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Filters

API 필터를 사용하여 ListTasks에 의해 반환되는 리소스 목록의 범위를 좁힐 수 있습니다. 예를 들어 특정 소스 위치의 모든 작업을 검색하려면 필터 이름 LocationId(와)과 해당 위치의 ARN Operator Equals(을)를 ListTasks(와)과 함께 사용할 수 있습니다.

타입: TaskFilter객체 배열

필수: 아니요

MaxResults

반환할 최대 열 수입니다.

유형: 정수

유효 범위: 최소값은 0입니다. 최댓값은 100입니다.

필수 여부: 아니요

NextToken

다음 작업 목록을 시작할 위치를 나타내는 불투명한 문자열입니다.

유형: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: [a-zA-Z0-9=_-]+

필수 여부: 아니요

응답 구문

```
{
   "NextToken": "string",
   "Tasks": [
      {
         "Name": "string",
         "Status": "string",
         "TaskArn": "string",
         "TaskMode": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

다음 작업 목록 반환을 시작할 위치를 나타내는 불투명한 문자열입니다.

유형: 문자열

길이 제약 조건: 최대 길이는 65,535입니다.

패턴: [a-zA-Z0-9=_-]+

Tasks

반환되는 모든 작업의 목록입니다.

타입: TaskListEntry 객체 배열

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

StartTaskExecution

AWS DataSync 전송 작업을 시작합니다. 각 작업에 대해 한 번에 하나의 작업 실행만 수행할 수 있습니다.

작업 실행에는 여러 단계가 있습니다. 자세한 내용은 작업 실행 상태를 참조하십시오.

> **Important**
>
> Amazon S3 위치와 데이터를 주고받을 계획이라면 시작하기 전에 DataSync가 S3 요청 요금에 미치는 영향 및 DataSync 요금 페이지를 검토하십시오.

구문 요청

```
{
   "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"
    }
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Excludes

작업에서 제외할 파일을 결정하는 필터 규칙 목록을 지정합니다. 목록에는 제외할 패턴으로 구성된 단일 필터 문자열이 포함됩니다. 패턴은 "|"(즉, 파이프)로 구분됩니다(예: `"/folder1|/folder2"`).

유형: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

Includes

작업 실행 중 포함시킬 파일을 결정하는 필터 규칙 목록을 지정합니다. 패턴에는 포함시킬 패턴으로 구성된 단일 필터 문자열을 포함해야 합니다. 패턴은 "|"(즉, 파이프)로 구분됩니다(예: `"/folder1|/folder2"`).

유형: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

ManifestConfig

DataSync에서 전송하려는 파일 또는 객체 목록인 매니페스트를 구성합니다. 자세한 내용과 구성 예제는 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

이 파라미터를 사용할 때는 발신자 자격 증명(DataSync를 사용하는 역할)에 `iam:PassRole` 권한이 있어야 합니다. AWSDataSyncFullAccess 정책에는 이 권한이 포함됩니다.

매니페스트 구성을 제거하려면 이 파라미터를 빈 값으로 지정합니다.

유형: ManifestConfig객체

필수 여부: 아니요

OverrideOptions

전송 작업이 구성된 방식을 나타냅니다. 이러한 옵션에는 DataSync가 전송 중에 파일, 객체 및 관련 메타데이터 처리 방법이 포함됩니다. 또한 다른 옵션 중에서 데이터 무결성을 확인하고, 작업에 대한 대역폭 제한 설정 방법을 지정할 수 있습니다.

각 옵션에는 기본값이 있습니다. 필요한 경우가 아니라면 StartTaskExecution을 호출하기 전에 이러한 옵션을 구성하지 않아도 됩니다.

각 작업 실행에 대해 작업 옵션을 재정의할 수도 있습니다. 예를 들어 개별 실행에 대해 `LogLevel`을 조정할 수 있습니다.

유형: Options객체

필수 여부: 아니요

Tags

작업 실행을 나타내는 Amazon 리소스 이름(ARN)에 적용할 태그를 지정합니다.

태그는 DataSync 리소스를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 페어입니다.

유형: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 아니요

TaskArn

시작할 작업의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

필수 여부: 예

TaskReportConfig

DataSync 전송에 대한 세부 정보를 제공하는 작업 보고서를 구성할 방법을 지정합니다. 자세한 내용은 Monitoring your DataSync transfers with task reports 섹션을 참조하세요.

이 파라미터를 사용할 때는 발신자 자격 증명(DataSync를 사용하는 역할)에 `iam:PassRole` 권한이 있어야 합니다. AWSDataSyncFullAccess 정책에는 이 권한이 포함됩니다.

작업 보고서 구성을 제거하려면 이 파라미터를 비어 있음으로 지정합니다.

유형: TaskReportConfig객체

필수 항목 여부: 아니요

응답 구문

```
{
   "TaskExecutionArn": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

TaskExecutionArn

수행 중인 작업 실행의 ARN입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

예

예 요청

다음 예제에서는 지정된 작업의 기본 옵션을 사용하여 작업 실행을 시작합니다.

```
{
    "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"
}
```

샘플 응답

이 예제에서는 StartTaskExecution의 한 가지 사용법을 보여줍니다.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

TagResource

AWS 리소스에 태그를 적용합니다. 태그는 귀하의 리소스를 관리, 필터링 및 검색하는 데 도움이 되는 키-값 쌍입니다.

여기에는 위치, 작업 및 작업 실행과 같은 AWS DataSync 리소스가 포함됩니다.

구문 요청

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

ResourceArn

태그를 적용할 리소스의 Amazon 리소스 이름(ARN) 을 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(((agent|task|location)/(agent|task|loc)-[a-z0-9]{17}(/execution/exec-[a-f0-9]{17})?)|(system/storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}(/job/discovery-job-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})?))$`

필수 여부: 예

Tags

귀하가 리소스에 적용하고자 하는 태그를 지정합니다.

타입: TagListEntry객체 배열

배열 구성원: 최소수는 0개입니다. 최대수 50개.

필수 여부: 예

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UntagResource

AWS 리소스에서 태그를 제거합니다.

구문 요청

```
{
   "Keys": [ "string" ],
   "ResourceArn": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Keys

태에서 제거하려는 키를 지정합니다.

타입: 문자열 배열

배열 멤버: 최소수는 1개입니다. 최대수 50개.

길이 제약: 최소 길이 1. 최대 길이는 256입니다.

패턴: ^[a-zA-Z0-9\s+=._:/-]+$

필수 여부: 예

ResourceArn

태그를 제거할 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: ^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(((agent|task|location)/(agent|task|loc)-[a-z0-9]{17}(/execution/exec-[a-f0-9]{17})?)|(system/storage-system-[a-f0-9]{8}-

`[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}(/job/discovery-job-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})?))$`

필수 여부: 예

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS SDK for Ruby V3

UpdateAgent

AWS DataSync 에이전트의 이름을 업데이트합니다.

구문 요청

```
{
   "AgentArn": "string",
   "Name": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArn

업데이트할 에이전트의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 예

Name

에이전트를 구성하기 위해 사용하고자 하는 이름.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationAzureBlob

사용 중인 Microsoft Azure Blob 스토리지 전송 위치의 다음 구성을 수정합니다 AWS DataSync.

자세한 내용은 Azure Blob 스토리지를 사용하는 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "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"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccessTier

객체 또는 파일이 전송되어야 할 액세스 계층을 지정합니다. 이는 해당 위치를 전송 대상으로 사용하는 경우에만 적용됩니다. 자세한 내용은 액세스 티어를 참조하세요.

타입: 문자열

유효 값: `HOT | COOL | ARCHIVE`

필수 여부: 아니요

AgentArns

(선택 사항) 사용자 Azure Blob 스토리지 컨테이너와 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)을 지정합니다. 에이전트 없는 클라우드 간 전송을 설정하는 경우 이 파라미터에 값을 지정할 필요가 없습니다.

하나 이상의 에이전트를 지정할 수 있습니다. 자세한 내용은 전송에 복수 에이전트 사용을 참조하세요.

> **Note**
>
> 에이전트를 처음 생성한 후에는 스토리지 위치에서 에이전트를 추가하거나 제거할 수 없습니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

AuthenticationType

DataSync가 Azure Blob Storage에 액세스하는 데 사용하는 인증 방법을 지정합니다. DataSync는 공유 액세스 서명(SAS)을 사용하여 블롭 스토리지에 액세스할 수 있습니다.

타입: 문자열

유효 값: `SAS | NONE`

필수 여부: 아니요

BlobType

개체 또는 파일을 Azure Blob Storage로 전송할 때 사용할 블롭 유형을 지정합니다. 현재 DataSync는 데이터를 블록으로 Azure Blob Storage로 이동하는 것만 지원합니다. 블롭 유형에 대한 자세한 내용은 Azure Blob Storage 설명서를 참조하세요.

타입: 문자열

유효 값: BLOCK

필수 여부: 아니요

CmkSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 지정하며, 여기에는 DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트와 고객 관리형 AWS KMS key가 포함됩니다.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트, 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할과 같은 고객 관리형 보안 암호의 구성 정보를 지정합니다.

유형: CustomSecretConfig객체

필수 여부: 아니요

LocationArn

업데이트하는 Azure Blob Storage 전송 위치의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

SasConfiguration

DataSync가 Azure Blob Storage에 액세스할 수 있도록 허용하는 SAS 구성을 지정합니다.

유형: AzureBlobSasConfiguration객체

필수 여부: 아니요

Subdirectory

컨테이너의 가상 디렉터리로의 전송을 제한하려는 경우(예:/my/images) 경로 세그먼트를 지정합니다.

유형: 문자열

길이 제약: 최대 길이 1024.

패턴: ^[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}\p{C}]*$

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++

- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationEfs

사용 중인 Amazon EFS 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 Amazon EFS를 사용하는 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "AccessPointArn": "string",
   "FileSystemAccessRoleArn": "string",
   "InTransitEncryption": "string",
   "LocationArn": "string",
   "Subdirectory": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccessPointArn

DataSync가 Amazon EFS 파일 시스템을 탑재하는 데 사용하는 액세스 포인트의 Amazon 리소스 이름(ARN)을 지정합니다.

자세한 내용은 제한된 Amazon EFS 파일 시스템 액세스 섹션을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `(^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$)|(^$)`

필수 여부: 아니요

FileSystemAccessRoleArn

DataSync가 Amazon EFS 파일 시스템에 액세스할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할을 지정합니다.

이 역할 생성에 대한 자세한 내용은 Amazon EFS 파일 시스템 액세스를 위한 DataSync IAM 역할 생성을 참조하세요.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `(^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$)|(^$)`

필수 여부: 아니요

InTransitEncryption

DataSync가 Amazon EFS 파일 시스템으로 또는 파일 시스템에서 데이터를 전송할 때 Transport Layer Security(TLS) 1.2 암호화를 사용할지 여부를 지정합니다.

`AccessPointArn`을 사용하여 액세스 지점을 지정하거나 `FileSystemAccessRoleArn`을 사용하여 IAM 역할을 지정하는 경우 이 파라미터를 `TLS1_2`로 설정해야 합니다.

타입: 문자열

유효 값: `NONE | TLS1_2`

필수 여부: 아니요

LocationArn

업데이트하려는 Amazon EFS 전송 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

Subdirectory

Amazon EFS 파일 시스템에 대한 탑재 경로를 지정합니다. DataSync가 파일 시스템의 데이터를 읽거나 쓰는 위치입니다(소스 위치인지 대상 위치인지에 따라 다름).

기본적으로 DataSync는 루트 디렉터리(또는 사용자가 AccessPointArn을 사용하여 루트 디렉터리를 제공하는 경우 액세스 포인트)를 사용합니다. 전방향 슬래시(예: /path/to/folder)를 사용하여 하위 디렉터리를 포함할 수도 있습니다.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: ^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2

- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationFsxLustre

사용 중인 Amazon FSx for Lustre 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 Amazon FSx for Lustre를 사용하는 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "LocationArn": "string",
   "Subdirectory": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

업데이트하려는 FSx for Lustre 전송 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

Subdirectory

FSx for Lustre 파일 시스템에 대한 탑재 경로를 지정합니다. 경로에는 하위 디렉터리가 포함될 수 있습니다.

위치가 소스로 사용되는 경우 DataSync는 마운트 경로에서 데이터를 읽습니다. 위치가 대상으로 사용되는 경우 DataSync는 데이터를 탑재 경로에 기록합니다. 이 파라미터를 포함하지 않으면 DataSync는 파일 시스템의 루트 디렉터리(/)를 사용합니다.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK

- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationFsxOntap

사용 중인 Amazon FSx for NetApp ONTAP 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 FSx for ONTAP을 사용하는 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "LocationArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "CmkSecretConfig": {
            "KmsKeyArn": "string",
            "SecretArn": "string"
         },
         "CustomSecretConfig": {
            "SecretAccessRoleArn": "string",
            "SecretArn": "string"
         },
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "Subdirectory": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

업데이트하려는 FSx for ONTAP 전송 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

Protocol

DataSync가 Amazon FSx 파일 시스템에 액세스하는 데 사용하는 데이터 전송 프로토콜을 지정합니다.

유형: FsxUpdateProtocol객체

필수 여부: 아니요

Subdirectory

데이터를 주고 받을 스토리지 가상 머신(SVM)에 파일 공유 경로를 지정합니다.

정션 경로(탑재 지점이라고도 함), qtree 경로(NFS 파일 공유의 경우) 또는 공유 이름(SMB 파일 공유의 경우)을 지정할 수 있습니다. 예를 들어, 탑재 경로는 `/vol1`, `/vol1/tree1`또는 `/share1`일 수 있습니다.

> **Note**
>
> SVM의 루트 볼륨에 정션 경로를 지정하지 않습니다. 자세한 설명은 Amazon FSx for NetApp ONTAP User Guide(Amazon FSx for NetApp ONTAP 사용자 가이드)의 Managing FSx for ONTAP storage virtual machines(FSx for ONTAP 스토리지 가상 머신 관리)를 참조하세요.

타입: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationFsxOpenZfs

사용 중인 Amazon FSx for OpenZFS 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 FSx for OpenZFS를 사용하는 DataSync 전송 구성을 참조하세요.

> **Note**
>
> SMB와 관련된 요청 파라미터는 `UpdateLocationFsxOpenZfs`작업에서 지원되지 않습니다.

구문 요청

```
{
   "LocationArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "CmkSecretConfig": {
            "KmsKeyArn": "string",
            "SecretArn": "string"
         },
         "CustomSecretConfig": {
            "SecretAccessRoleArn": "string",
            "SecretArn": "string"
         },
         "Domain": "string",
         "ManagedSecretConfig": {
            "SecretArn": "string"
         },
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "Subdirectory": "string"
```

```
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

업데이트하려는 FSx for OpenZFS 전송 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

Protocol

가 Amazon FSx 파일 시스템에 액세스하는 데 AWS DataSync 사용하는 데이터 전송 프로토콜을 지정합니다.

유형: FsxProtocol객체

필수 여부: 아니요

Subdirectory

`/fsx`로 시작해야 하는 위치 경로의 하위 디렉터리를 지정합니다. DataSync는 이 하위 디렉터리를 사용하여 데이터를 읽거나 씁니다(파일 시스템이 소스 위치인지 목적지 위치인지에 따라 다름).

타입: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationFsxWindows

사용 중인 Amazon FSx for Windows File Server 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 FSx for Windows File Server를 사용한 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "Domain": "string",
   "LocationArn": "string",
   "Password": "string",
   "Subdirectory": "string",
   "User": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

CmkSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 DataSync 사용하는 Password 또는 자격 증명 세트와 고객 관리형 보안 암호에 대한 구성 정보를 지정합니다 AWS KMS key.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 사용하는 Password 또는 자격 증명 세트와 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할과 같은 고객 관리형 보안 암호의 구성 정보를 지정합니다.

유형: CustomSecretConfig객체

필수 여부: 아니요

Domain

FSx for Windows File Server 파일 시스템이 속한 Windows 도메인의 이름을 지정합니다.

환경에 여러 Active Directory 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 파일 시스템에 연결되게 할 수 있습니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^([A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252})?$`

필수 여부: 아니요

LocationArn

업데이트하려는 FSx for Windows File Server 전송 위치의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

Password

FSx for Windows File Server 파일 시스템의 파일, 폴더, 파일 메타데이터를 탑재하고 이에 액세스할 수 있는 권한이 있는 사용자의 암호를 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^.{0,104}$`

필수 여부: 아니요

Subdirectory

슬래시를 사용하여 파일 시스템에 대한 탑재 경로를 지정합니다. DataSync는 이 하위 디렉터리를 사용하여 데이터를 읽거나 씁니다(파일 시스템이 소스 위치인지 목적지 위치인지에 따라 다름).

타입: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

User

FSx for Windows File Server 파일 시스템의 파일, 폴더, 파일 메타데이터를 탑재하고 이에 액세스할 수 있는 권한이 있는 사용자를 지정합니다.

전송에 적합한 수준의 액세스 권한을 가진 사용자를 선택하는 방법에 대한 자세한 내용은 FSx for Windows File Server 위치에 필요한 권한을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationHdfs

사용 중인 Hadoop 분산 파일 시스템(HDFS) 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 HDFS 클러스터를 사용하는 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlockSize": number,
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "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"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArns

HDFS 클러스터에 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

AuthenticationType

사용자 ID를 결정하는 데 사용되는 인증 타입.

타입: 문자열

유효 값: `SIMPLE | KERBEROS`

필수 여부: 아니요

BlockSize

HDFS 클러스터에 쓸 데이터 블록의 크기입니다.

타입: 정수

유효한 범위: 최소값은 1048576입니다. 최대값은 1073741824입니다.

필수 여부: 아니요

CmkSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 DataSync 사용하는 `KerberosKeytab` 또는 자격 증명 세트와 고객 관리형 보안 암호에 대한 구성 정보를 지정합니다 AWS KMS key.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 사용하는 KerberosKeytab 또는 자격 증명 세트와 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할과 같은 고객 관리형 보안 암호의 구성 정보를 지정합니다.

유형: CustomSecretConfig객체

필수 여부: 아니요

KerberosKeytab

정의된 Kerberos 보안 주체와 암호화된 키 간의 매핑이 포함된 Kerberos 키 테이블(keytab)입니다. 파일 주소를 제공하여 파일에서 키탭을 로드할 수 있습니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 65536입니다.

필수 여부: 아니요

KerberosKrb5Conf

Kerberos 구성 정보가 포함된 krb5.conf 파일입니다. 파일 주소를 제공하여 krb5.conf파일을 로드할 수 있습니다. AWS CLI를 사용하는 경우, base64 인코딩을 자동으로 수행합니다. 그렇지 않으면 base64 인코딩 형식의 텍스트를 제공하십시오.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 131072입니다.

필수 여부: 아니요

KerberosPrincipal

HDFS 클러스터의 파일 및 폴더에 대한 액세스 권한이 있는 Kerberos 보안 주체입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: ^.+$

필수 여부: 아니요

KmsKeyProviderUri

HDFS 클러스터의 키 관리 서버(KMS)의 URI입니다.

타입: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 255.

패턴: `^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$`

필수 여부: 아니요

LocationArn

소스 HDFS 클러스터 위치의 Amazon 리소스 이름(ARN)입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

NameNodes

HDFS 네임스페이스를 관리하는 NameNode입니다. NameNode는 파일 및 디렉터리 열기, 닫기 및 이름 바꾸기와 같은 작업을 수행합니다. NameNode에는 데이터 블록을 DataNode에 매핑하기 위한 정보가 들어 있습니다. 하나의 NameNode만 사용할 수 있습니다.

타입: HdfsNameNode객체 배열

배열 구성원: 최소수는 1개입니다.

필수 여부: 아니요

QopConfiguration

QOP(Quality of Protection) 구성은 Hadoop 분산 파일 시스템(HDFS) 클러스터에 구성된 원격 프로시저 호출(RPC) 및 데이터 전송 개인 정보 보호 설정을 지정합니다.

타입: QopConfiguration객체

필수 여부: 아니요

ReplicationFactor

HDFS 클러스터에 쓸 때 데이터를 복제할 DataNode의 수입니다.

타입: 정수

유효 범위: 최소값 1. 최대값은 512입니다.

필수 여부: 아니요

SimpleUser

호스트 운영 체제에서 클라이언트를 식별하는 데 사용되는 사용자 이름입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

필수 여부: 아니요

Subdirectory

HDFS 클러스터의 하위 디렉터리입니다. 이 하위 디렉터리는 HDFS 클러스터에서 데이터를 읽거나 쓰는 데 사용됩니다.

타입: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationNfs

사용 중인 NFS(Network File System) 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 NFS 파일 서버를 사용하는 전송 구성을 참조하세요.

구문 요청

```
{
   "LocationArn": "string",
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
   },
   "ServerHostname": "string",
   "Subdirectory": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

업데이트하려는 NFS 전송 위치의 Amazon 리소스 이름(ARN) 을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

MountOptions

DataSync가 NFS 프로토콜을 사용하여 위치에 액세스하는 방법을 지정합니다.

타입: NfsMountOptions객체

필수 여부: 아니요

OnPremConfig

NFS(Network File System) 파일 서버에 연결할 수 있는 AWS DataSync 에이전트입니다.

유형: OnPremConfig객체

필수 여부: 아니요

ServerHostname

DataSync 에이전트가 연결될 NFS 파일 서버의 DNS 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

필수 여부: 아니요

Subdirectory

DataSync에서 탑재할 NFS 파일 서버의 내보내기 경로를 지정합니다.

이 경로(또는 경로의 하위 디렉터리)는 DataSync가 데이터를 전송하고 전송 받는 곳입니다. DataSync용 내보내기 구성에 대한 자세한 내용은 NFS 파일 서버 액세스를 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]+$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationObjectStorage

사용 중인 객체 스토리지 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 객체 스토리지 시스템을 사용하는 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "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"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccessKey

객체 스토리지 서버에 인증하는 데 자격 증명이 필요한 경우, 액세스 키(예: 사용자 이름)를 지정합니다.

유형: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: ^.*$

필수 여부: 아니요

AgentArns

(선택 사항) 객체 스토리지 시스템과 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)을 지정합니다. 에이전트 없는 클라우드 간 전송을 설정하는 경우 이 파라미터에 값을 지정할 필요가 없습니다.

> **Note**
>
> 에이전트를 처음 생성한 후에는 스토리지 위치에서 에이전트를 추가하거나 제거할 수 없습니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

CmkSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 지정하며, 여기에는 DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트와 고객 관리형 AWS KMS key가 포함됩니다.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트, 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할과 같은 고객 관리형 보안 암호의 구성 정보를 지정합니다.

유형: CustomSecretConfig객체

필수 여부: 아니요

LocationArn

업데이트하려는 오브젝트 스토리지 시스템 위치의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

SecretKey

객체 스토리지 서버에 인증하는 데 자격 증명이 필요한 경우, 보안 암호 키(예: 암호)를 지정합니다.

> **Note**
>
> 를 사용하여 보안 암호를 제공`SecretKey`하지만 `CmkSecretConfig` 또는를 사용하여 보안 암호 구성 세부 정보를 제공하지 않는 경우 `CustomSecretConfig` DataSync는 AWS 계정의 Secrets Manager 보안 암호를 사용하여 토큰을 저장합니다.

유형: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: `^.*$`

필수 여부: 아니요

ServerCertificate

시스템이 프라이빗 또는 자체 서명 인증 기관(CA)을 사용하는 경우 DataSync가 객체 스토리지 시스템으로 인증하기 위한 인증서 체인을 지정합니다. 전체 인증서 체인(예: `file:///home/user/.ssh/object_storage_certificates.pem`)이 있는 단일 `.pem` 파일을 지정해야 합니다.

인증서 체인에는 다음이 포함될 수 있습니다.

- 객체 스토리지 시스템의 인증서

- 모든 중간 인증서(있는 경우)
- 서명 CA의 루트 인증서

인증서를 `.pem` 파일로 연결할 수 있습니다(base64 인코딩 전 최대 32,768바이트). 다음 예제의 `cat` 명령은 세 개의 인증서가 포함된 `object_storage_certificates.pem` 파일을 생성합니다.

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

이 파라미터를 사용하려면(`ServerProtocol`을)를(`HTTPS`으)로 구성하세요.

이 파라미터를 업데이트해도 진행 중인 작업은 방해되지 않습니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 32768입니다.

필수 여부: 아니요

ServerHostname

DataSync 에이전트가 연결될 객체 스토리지 서버의 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

필수 여부: 아니요

ServerPort

객체 스토리지 서버가 인바운드 네트워크 트래픽을 수락하는 포트(예: 포트 443)를 지정합니다.

타입: 정수

유효 범위: 최소값 1. 최대값은 65536입니다.

필수 여부: 아니요

ServerProtocol

객체 스토리지 서버의 통신에 사용되는 프로토콜을 지정합니다.

타입: 문자열

유효 값: HTTPS | HTTP

필수 여부: 아니요

Subdirectory

객체 스토리지 서버의 객체 접두사를 지정합니다. 소스 위치인 경우, DataSync는 이 접두사가 있는 객체만 복사합니다. 목적지 위치인 경우, DataSync는 이 접두사가 있는 모든 객체를 씁니다.

타입: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: ^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationS3

사용 중인 Amazon S3 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

> **Important**
>
> 시작하기 전에 다음 주제를 읽어보시기 바랍니다.
>
> - Amazon S3 위치의 스토리지 클래스 고려 사항
> - DataSync 사용 시 S3 요청 비용 평가

구문 요청

```
{
   "LocationArn": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
   "S3StorageClass": "string",
   "Subdirectory": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

LocationArn

업데이트하려는 Amazon S3 전송 위치의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

S3Config

DataSync가 S3 버킷에 액세스하는 데 사용하는 (IAM) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (ARN)을 지정합니다.

자세한 내용은 DataSync에 S3 버킷 액세스 권한 제공을 참조하세요.

유형: S3Config객체

필수 여부: 아니요

S3StorageClass

Amazon S3가 전송 대상일 때 객체가 사용할 스토리지 클래스를 지정합니다.

의 버킷 AWS 리전의 경우 스토리지 클래스의 기본값은 입니다STANDARD. 의 버킷 AWS Outposts 의 경우 스토리지 클래스의 기본값은 입니다OUTPOSTS.

자세한 내용은 Storage class considerations with Amazon S3 transfers 섹션을 참조하세요.

타입: 문자열

유효 값: `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

필수 여부: 아니요

Subdirectory

DataSync가 읽거나 쓰는 S3 버킷의 접두사를 입력합니다(버킷이 소스인지 대상 위치인지에 따라 다름).

> **Note**
>
> DataSync는 슬래시(/)로 시작하거나 `//`, `/./` 또는 `/../` 패턴을 포함하는 접두사가 있는 객체를 전송할 수 없습니다. 예제:
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`
> - `photos/../2006/March`

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateLocationSmb

사용 중인 SMB(Server Message Block) 전송 위치의 다음 구성 파라미터를 수정합니다 AWS DataSync.

자세한 내용은 SMB 파일 서버를 사용하는 DataSync 전송 구성을 참조하세요.

구문 요청

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosKeytab": blob,
   "KerberosKrb5Conf": blob,
   "KerberosPrincipal": "string",
   "LocationArn": "string",
   "MountOptions": {
      "Version": "string"
   },
   "Password": "string",
   "ServerHostname": "string",
   "Subdirectory": "string",
   "User": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

AgentArns

SMB 파일 서버에 연결할 수 있는 DataSync 에이전트(또는 에이전트들)를 지정합니다. 에이전트의 Amazon 리소스 이름(ARN)을 사용하여 에이전트를 지정합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

AuthenticationType

DataSync가 SMB 파일 서버에 연결하는 데 사용하는 인증 프로토콜을 지정합니다. DataSync는 `NTLM`(기본값) 및 `KERBEROS` 인증을 지원합니다.

자세한 내용은 DataSync에 SMB 파일 서버 액세스 권한 제공을 참조하세요.

타입: 문자열

유효 값: `NTLM | KERBEROS`

필수 여부: 아니요

CmkSecretConfig

DataSync가 특정 전송 위치 및 고객 관리형에 액세스하는 데 사용하는 `Password` `KerberosKeytab` 또는 자격 증명 세트와 같은 DataSync 관리형 보안 암호의 구성 정보를 지정합니다 AWS KMS key.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 사용하는 `Password` `KerberosKeytab` 또는 자격 증명 세트와 보안 암호에 대한 액세스를 제공하는 고객 관리형 AWS Identity and Access Management (IAM) 역할과 같은 고객 관리형 보안 암호의 구성 정보를 지정합니다.

유형: CustomSecretConfig객체

필수 여부: 아니요

DnsIpAddresses

SMB 파일 서버가 속한 DNS 서버의 IP 주소(IPv4 또는 IPv6)를 지정합니다. 이 파라미터는 `AuthenticationType`이 `KERBEROS`로 설정된 경우에만 적용됩니다.

환경에 여러 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 SMB 파일 서버에 연결되도록 할 수 있습니다.

유형: 문자열 배열

배열 멤버: 최대 항목 수는 2개입니다.

길이 제약: 최소 길이는 7입니다. 최대 길이는 39입니다.

패턴: `\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`

필수 여부: 아니요

Domain

SMB 파일 서버가 속한 Windows 도메인 이름을 지정합니다. 이 파라미터는 `AuthenticationType`이 `NTLM`로 설정된 경우에만 적용됩니다.

환경에 여러 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 파일 서버에 연결되도록 할 수 있습니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

필수 여부: 아니요

KerberosKeytab

Kerberos 보안 주체와 암호화 키 간의 매핑을 포함하는 Kerberos 키 테이블(keytab) 파일을 지정합니다.

작업 실행 오류를 방지하려면 키탭 파일을 생성하는 데 사용하는 Kerberos 보안 주체가 `KerberosPrincipal`에 지정한 것과 정확히 일치하는지 확인합니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 65536입니다.

필수 여부: 아니요

KerberosKrb5Conf

Kerberos 영역 구성을 정의하는 Kerberos 구성 파일(`krb5.conf`)을 지정합니다.

파일은 반드시 base64로 인코딩되어야 합니다. 를 사용하는 경우 AWS CLI인코딩이 수행됩니다.

타입: Base64로 인코딩된 이진 데이터 객체

길이 제약: 최대 길이는 131072입니다.

필수 여부: 아니요

KerberosPrincipal

Kerberos 영역에서 SMB 파일 서버의 파일, 폴더, 파일 메타데이터에 액세스할 수 있는 권한을 가진 Kerberos 보안 주체를 지정합니다.

Kerberos 보안 주체는 `HOST/kerberosuser@MYDOMAIN.ORG`처럼 보일 수 있습니다.

보안 주체 이름은 대/소문자를 구분합니다. 이 파라미터에 대해 지정한 보안 주체가 키탭 파일 생성에 사용하는 보안 주체와 정확히 일치하지 않으면 DataSync 작업 실행이 실패합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^.+$`

필수 여부: 아니요

LocationArn

업데이트하려는 SMB 위치의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 예

MountOptions

가 SMB 파일 서버에 액세스하는 데 AWS DataSync 사용하는 SMB(Server Message Block) 프로토콜의 버전을 지정합니다.

유형: SmbMountOptions객체

필수 여부: 아니요

Password

사용자 SMB 파일 서버를 탑재하고 전송과 관련된 파일과 폴더에 액세스할 수 있는 권한이 있는 사용자의 암호를 지정합니다. 이 파라미터는 `AuthenticationType`이 `NTLM`로 설정된 경우에만 적용됩니다.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^.{0,104}$`

필수 여부: 아니요

ServerHostname

DataSync 에이전트가 연결될 SMB 파일 서버의 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다.

> **Note**
>
> Kerberos 인증을 사용하는 경우 도메인 이름을 지정해야 합니다.

유형: 문자열

길이 제약: 최대 길이는 255입니다.

패턴: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

필수 여부: 아니요

Subdirectory

DataSync가 데이터를 읽거나 쓸 SMB 파일 서버에서 내보낸 공유의 이름을 지정합니다. 공유 경로에 하위 디렉토리(예: `/path/to/subdirectory`)를 포함할 수 있습니다. 네트워크의 다른 SMB 클라이언트도 이 경로를 마운트할 수 있는지 확인하세요.

지정된 하위 디렉터리의 모든 데이터를 복사하려면 DataSync가 SMB 공유를 탑재하고 모든 데이터에 액세스할 수 있어야 합니다. 자세한 내용은 DataSync에 SMB 파일 서버 액세스 권한 제공을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

필수 여부: 아니요

User

SMB 파일 서버를 탑재할 수 있는 사용자 이름을 지정하고 전송과 관련된 파일 및 폴더에 액세스할 권한이 있는 사용자 이름을 지정합니다. 이 파라미터는 `AuthenticationType`이 `NTLM`로 설정된 경우에만 적용됩니다.

전송에 적합한 수준의 액세스 권한을 가진 사용자를 선택하는 방법에 대한 자세한 내용은 SMB 파일 서버에 대한 DataSync 액세스 제공을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateTask

AWS DataSync 이 데이터를 이동하는 위치와 방법을 정의하는 작업의 구성을 업데이트합니다.

구문 요청

```
{
   "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"
   }
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

CloudWatchLogGroupArn

작업을 모니터링하기 위한 Amazon CloudWatch 로그 그룹의 Amazon 리소스 이름(ARN)을 지정합니다.

확장 모드 작업의 경우 `/aws/datasync`를 로그 그룹 이름으로 사용해야 합니다. 예제:

`arn:aws:logs:us-east-1:111222333444:log-group:/aws/datasync:*`

자세한 내용은 CloudWatch Logs를 사용하여 데이터 전송 모니터링을 참조하세요.

유형: 문자열

길이 제약 조건: 최대 길이는 562입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

필수 여부: 아니요

Excludes

DataSync가 전송하지 않도록 소스 위치의 파일, 객체 및 폴더를 정의하는 제외 필터를 지정합니다. 자세한 내용과 예제는 Specifying what DataSync transfers by using filters 섹션을 참조하세요.

타입: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

Includes

DataSync가 전송하도록 소스 위치의 파일, 객체 및 폴더를 정의하는 포함 필터를 지정합니다. 자세한 내용과 예제는 Specifying what DataSync transfers by using filters 섹션을 참조하세요.

타입: FilterRule객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

ManifestConfig

DataSync에서 전송하려는 파일 또는 객체 목록인 매니페스트를 구성합니다. 자세한 내용과 구성 예제는 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

이 파라미터를 사용할 때는 발신자 자격 증명(DataSync를 사용하는 IAM 역할)에 `iam:PassRole` 권한이 있어야 합니다. AWSDataSyncFullAccess 정책에는 이 권한이 포함됩니다.

매니페스트 구성을 제거하려면 이 파라미터를 비어 있음으로 지정합니다.

유형: ManifestConfig객체

필수 여부: 아니요

Name

작업의 이름을 지정합니다.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

Options

전송 작업이 구성된 방식을 나타냅니다. 이러한 옵션에는 DataSync가 전송 중에 파일, 객체 및 관련 메타데이터 처리 방법이 포함됩니다. 또한 다른 옵션 중에서 데이터 무결성을 확인하고, 작업에 대한 대역폭 제한 설정 방법을 지정할 수 있습니다.

각 옵션에는 기본값이 있습니다. 필요한 경우가 아니라면 StartTaskExecution을 호출하기 전에 이러한 옵션을 구성하지 않아도 됩니다.

각 작업 실행에 대해 작업 옵션을 재정의할 수도 있습니다. 예를 들어 개별 실행에 대해 `LogLevel`을 조정할 수 있습니다.

유형: Options객체

필수 여부: 아니요

Schedule

작업을 실행할 일정을 지정합니다. 자세한 내용을 알아보려면 태스크 예약을 참조하십시오.

유형: TaskSchedule객체

필수 여부: 아니요

TaskArn

업데이트하려는 작업의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

필수 여부: 예

TaskReportConfig

DataSync 전송에 대한 세부 정보를 제공하는 작업 보고서를 구성할 방법을 지정합니다. 자세한 내용은 Monitoring your DataSync transfers with task reports 섹션을 참조하세요.

이 파라미터를 사용할 때는 발신자 자격 증명(DataSync를 사용하는 IAM 역할)에 `iam:PassRole` 권한이 있어야 합니다. AWSDataSyncFullAccess 정책에는 이 권한이 포함됩니다.

작업 보고서 구성을 제거하려면 이 파라미터를 비어 있음으로 지정합니다.

유형: TaskReportConfig객체

필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

UpdateTaskExecution

실행 중인 AWS DataSync 작업 실행의 구성을 업데이트합니다.

> **Note**
>
> UpdateTaskExecution를 사용하여 현재 수정할 수 있는 유일한 Option은 BytesPerSecond 으로 실행 중이거나 대기중인 작업 실행의 대역폭을 제한하는 것입니다.

구문 요청

```
{
   "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"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 자세한 설명은 공통 파라미터를 참조하세요.

요청은 JSON 형식으로 다음 데이터를 받습니다.

Options

전송 작업이 구성된 방식을 나타냅니다. 이러한 옵션에는 DataSync가 전송 중에 파일, 객체 및 관련 메타데이터 처리 방법이 포함됩니다. 또한 다른 옵션 중에서 데이터 무결성을 확인하고, 작업에 대한 대역폭 제한 설정 방법을 지정할 수 있습니다.

각 옵션에는 기본값이 있습니다. 필요한 경우가 아니라면 StartTaskExecution을 호출하기 전에 이러한 옵션을 구성하지 않아도 됩니다.

각 작업 실행에 대해 작업 옵션을 재정의할 수도 있습니다. 예를 들어 개별 실행에 대해 `LogLevel`을 조정할 수 있습니다.

타입: Options객체

필수 항목 여부: 예

TaskExecutionArn

업데이트하려는 태스크 실행의 Amazon 리소스 이름(ARN) 을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

필수 여부: 예

응답 요소

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 설명은 일반적인 오류 유형섹션을 참조하세요.

InternalException

이 예외는 AWS DataSync 서비스에 오류가 발생할 때 던져집니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS 명령줄 인터페이스 V2
- AWS .NET V4용 SDK
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

데이터 타입

다음 데이터 타입이 지원됩니다.

- AgentListEntry
- AzureBlobSasConfiguration
- CmkSecretConfig
- CustomSecretConfig
- Ec2Config
- FilterRule
- FsxProtocol
- FsxProtocolNfs
- FsxProtocolSmb

- FsxUpdateProtocol
- FsxUpdateProtocolSmb
- HdfsNameNode
- LocationFilter
- LocationListEntry
- ManagedSecretConfig
- ManifestConfig
- NfsMountOptions
- OnPremConfig
- Options
- Platform
- PrivateLinkConfig
- QopConfiguration
- ReportDestination
- ReportDestinationS3
- ReportOverride
- ReportOverrides
- ReportResult
- S3Config
- S3ManifestConfig
- SmbMountOptions
- SourceManifestConfig
- TagListEntry
- TaskExecutionFilesFailedDetail
- TaskExecutionFilesListedDetail
- TaskExecutionFoldersFailedDetail
- TaskExecutionFoldersListedDetail
- TaskExecutionListEntry
- TaskExecutionResultDetail
- TaskFilter

- TaskListEntry
- TaskReportConfig
- TaskSchedule
- TaskScheduleDetails

AgentListEntry

ListAgents 작업을 호출할 때 AWS DataSync 에이전트 목록(또는 배열)의 단일 항목을 나타냅니다.

내용

AgentArn

DataSync 에이전트의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 아니요

Name

에이전트의 이름.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

Platform

에이전트에 대한 플랫폼 관련 세부 정보(예: 버전 번호)

유형: Platform객체

필수 여부: 아니요

Status

에이전트의 상태.

- 상태가 `ONLINE`이면 에이전트가 제대로 구성되어 사용할 준비가 된 것입니다.

- 상태가 OFFLINE이면 에이전트가 5분 이상 동안 DataSync와 연락이 끊긴 것입니다. 몇 가지 원인이 있을 수 있습니다. 자세한 내용은 에이전트가 오프라인 상태인 경우 어떻게 하나요? 를 확인하세요.

타입: 문자열

유효 값: ONLINE | OFFLINE

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

AzureBlobSasConfiguration

AWS DataSync이 사용자 Microsoft Azure Blob 스토리지에 액세스하게 해 주는 공유 액세스 서명(SAS) 구성입니다.

자세한 내용은 Azure Blob 스토리지에 액세스하기 위한 SAS 토큰을 참조하세요.

내용

Token

Azure Blob 스토리지에 액세스할 수 있는 권한을 제공하는 SAS 토큰을 지정합니다.

토큰은 스토리지 리소스 URI와 물음표 뒤에 오는 SAS URI 문자열의 일부입니다. 토큰은 다음과 같은 형태입니다:

```
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
```

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 255.

패턴: `^.+$`

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CmkSecretConfig

DataSync가 고객 관리형를 사용하여 특정 스토리지 위치에 액세스하는 데 사용하는 인증 토큰, 보안 암호 키, 암호 또는 Kerberos 키 탭과 같은 DataSync 관리형 보안 암호의 구성 정보를 지정합니다 AWS KMS key.

> **Note**
>
> `CmkSecretConfig` 또는 `CustomSecretConfig`을 사용하여 `CreateLocation` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

내용

KmsKeyArn

DataSync AWS KMS key 가에 대해 저장된 DataSync 관리형 보안 암호를 암호화하는 데 사용하는 고객 관리형 보안 암호의 ARN을 지정합니다`SecretArn`. DataSync는이 키를에 제공합니다 AWS Secrets Manager.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):kms:[a-z\-0-9]+:[0-9]{12}:key/.*|)$`

필수 여부: 아니요

SecretArn

특정 스토리지 위치에 액세스하는 데 사용되는 DataSync 관리형 AWS Secrets Manager 보안 암호의 ARN을 지정합니다. 이 속성은 DataSync에서 읽기 전용으로 생성됩니다. DataSync는 `KmsKeyArn`에 지정한 KMS 키로 이 보안 암호를 암호화합니다.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

CustomSecretConfig

스토리지 위치 보안 인증 정보가 Secrets Manager에 일반 텍스트(인증 토큰, 보안 키 또는 암호의 경우) 또는 바이너리(Kerberos 키 탭의 경우)로 저장되는 고객 관리형 Secrets Manager 보안 암호의 구성 정보를 지정합니다. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다.

> **Note**
>
> `CmkSecretConfig` 또는 `CustomSecretConfig`을 사용하여 `CreateLocation` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

내용

SecretAccessRoleArn

DataSync가에 지정된 보안 암호에 액세스하는 데 사용하는 AWS Identity and Access Management 역할의 ARN을 지정합니다`SecretArn`.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/[a-zA-Z0-9+=,.@_-]+|)$`

필수 여부: 아니요

SecretArn

AWS Secrets Manager 보안 암호의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

Ec2Config

가 Amazon EFS 파일 시스템의 탑재 대상 중 하나에 연결하는 데 AWS DataSync 사용하는 서브넷 및 보안 그룹입니다.

내용

SecurityGroupArns

Amazon EFS 파일 시스템의 탑재 대상과 연결된 보안 그룹의 Amazon 리소스 이름(ARN)을 지정합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수 5개.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

필수 여부: 예

SubnetArn

DataSync가 전송 중 트래픽 관리를 위한 네트워크 인터페이스를 생성하는 서브넷의 ARN을 지정합니다.

서브넷은 다음 위치에 있어야 합니다.

- Amazon EFS 파일 시스템과 동일한 Virtual Private Cloud(VPC)
- Amazon EFS 파일 시스템에 대한 하나 이상의 탑재 대상과 동일한 가용 영역

> **Note**
>
> 파일 시스템 탑재 대상을 포함하는 서브넷을 지정할 필요가 없습니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/subnet-[a-f0-9]+$`

필수 여부: 예

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

FilterRule

소스에서 대상으로 파일을 전송할 때 포함시키거나 제외시킬 파일, 폴더 및 객체를 지정합니다.

내용

FilterType

적용할 필터 규칙의 유형입니다. AWS DataSync는 SIMPLE_PATTERN 규칙 유형만 지원합니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^[A-Z0-9_]+$`

유효 값: `SIMPLE_PATTERN`

필수 여부: 아니요

Value

포함하거나 제외할 패턴으로 구성된 단일 필터 문자열입니다. 패턴은 "|" (즉, 파이프) 로 구분됩니다. 예를 들면 다음과 같습니다. `/folder1|/folder2`

유형: 문자열

길이 제약 조건: 최대 길이는 102,400입니다.

패턴: `^[^\x00]+$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FsxProtocol

AWS DataSync가 Amazon FSx 파일 시스템에 액세스하는 데 사용하는 데이터 전송 프로토콜을 지정합니다.

내용

NFS

DataSync가 FSx for OpenZFS 파일 시스템 또는 FSx for ONTAP 파일 시스템의 스토리지 가상 머신(SVM)에 액세스하는 데 사용하는 네트워크 파일 시스템(NFS) 프로토콜 구성을 지정합니다.

유형: FsxProtocolNfs객체

필수 여부: 아니요

SMB

DataSync가 FSx for ONTAP 파일 시스템의 SVM에 액세스하는 데 사용하는 Server Message Block(SMB) 프로토콜 구성을 지정합니다.

유형: FsxProtocolSmb객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FsxProtocolNfs

DataSync가 FSx for OpenZFS 파일 시스템 또는 FSx for ONTAP 파일 시스템의 스토리지 가상 머신(SVM)에 액세스하는 데 사용하는 네트워크 파일 시스템(NFS) 프로토콜 구성을 지정합니다.

내용

MountOptions

DataSync가 NFS 프로토콜을 사용하여 위치에 액세스하는 방법을 지정합니다.

타입: NfsMountOptions객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FsxProtocolSmb

가 Amazon FSx for NetApp ONTAP 파일 시스템의 스토리지 가상 머신(SVM)에 액세스하는 데 AWS DataSync 사용하는 서버 메시지 블록(SMB) 프로토콜 구성을 지정합니다. 자세한 내용은 DataSync에 FSx for ONTAP 파일 서버 액세스 권한 제공을 참조하세요.

내용

User

SVM에 파일, 폴더 및 메타데이터를 탑재하고 이에 액세스할 수 있는 사용자를 지정합니다.

전송에 적합한 수준의 액세스 권한을 가진 사용자를 선택하는 방법에 대한 자세한 내용은 SMB 프로토콜 사용을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

필수 여부: 예

CmkSecretConfig

DataSync 관리형 보안 암호에 대한 구성 정보를 지정합니다. 여기에는 DataSync가 고객 관리형 보안 암호로 특정 FSx for ONTAP 스토리지 위치(SMB 사용)에 액세스하는 데 사용하는 암호가 포함됩니다 AWS KMS key.

이 파라미터를 `CreateLocationFsxOntap` 요청의 일부로 포함하는 경우 KMS 키 ARN만 제공합니다. DataSync는 `Password`에 대해 지정한와 함께이 KMS 키를 사용하여 위치 액세스 자격 증명을 저장하는 DataSync 관리형 보안 암호를 생성합니다.

DataSync에 지정한 KMS 키에 액세스할 수 있는 권한이 있는지 확인합니다. 자세한 내용은 사용자 지정으로 암호화된 서비스 관리형 보안 암호 사용을 참조하세요 AWS KMS key.

> **Note**
>
> `CmkSecretConfig`(`Password` 포함) 또는 `CustomSecretConfig`(`Password` 제외)을 사용하여 `CreateLocationFsxOntap` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

FSx for ONTAP 스토리지 위치(SMB 사용)의 암호가 Secrets Manager에 일반 텍스트로 저장되는 고객 관리형 Secrets Manager 보안 암호의 구성 정보를 지정합니다. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다. 자세한 내용은 관리하는 보안 암호 사용을 참조하세요.

> **Note**
>
> `CmkSecretConfig`(`Password` 포함) 또는 `CustomSecretConfig`(`Password` 제외)을 사용하여 `CreateLocationFsxOntap` 요청에 대한 자격 증명을 제공할 수 있습니다. 같은 요청에 대해 두 파라미터를 모두 제공하지 마세요.

유형: CustomSecretConfig객체

필수 여부: 아니요

Domain

스토리지 가상 머신(SVM)이 속한 Windows 도메인의 이름을 지정합니다.

환경에 여러 도메인이 있는 경우 이 설정을 구성하면 DataSync가 올바른 SVM에 연결되게 할 수 있습니다.

환경에 여러 Active Directory 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 SVM에 연결되도록 할 수 있습니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

필수 여부: 아니요

ManagedSecretConfig

DataSync가 특정 스토리지 위치에 액세스하는 데 사용하는와 같은 `Password` DataSync 관리형 보안 암호의 구성 정보를 설명합니다. DataSync는 기본 AWS관리형 KMS 키를 사용하여이 보안 암호를 암호화합니다 AWS Secrets Manager.

> **Note**
>
> `CreateLocation` 요청에이 정보를 제공하지 마십시오. `ManagedSecretConfig`는 ReadOnly 속성이며 `DescribeLocation` 응답에만 채워집니다.

유형: ManagedSecretConfig객체

필수 여부: 아니요

MountOptions

가 SMB 파일 서버에 액세스하는 데 AWS DataSync 사용하는 SMB(Server Message Block) 프로토콜의 버전을 지정합니다.

유형: SmbMountOptions객체

필수 여부: 아니요

Password

SVM에 액세스할 수 있는 권한이 있는 사용자의 암호를 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^.{0,104}$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

FsxUpdateProtocol

AWS DataSync가 Amazon FSx 파일 시스템에 액세스하는 데 사용하는 데이터 전송 프로토콜을 지정합니다.

> **Note**
>
> FSx for ONTAP 위치에 대한 네트워크 파일 시스템(NFS) 프로토콜 구성은 업데이트할 수 없습니다. DataSync는 현재 이 위치 유형에 대해 NFS 버전 3만 지원합니다.

내용

NFS

DataSync가 FSx for OpenZFS 파일 시스템 또는 FSx for ONTAP 파일 시스템의 스토리지 가상 머신(SVM)에 액세스하는 데 사용하는 네트워크 파일 시스템(NFS) 프로토콜 구성을 지정합니다.

유형: FsxProtocolNfs객체

필수 여부: 아니요

SMB

DataSync가 FSx for ONTAP 파일 시스템의 스토리지 가상 머신(SVM)에 액세스하는 데 사용하는 SMB(Server Message Block) 프로토콜 구성을 지정합니다.

유형: FsxUpdateProtocolSmb객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FsxUpdateProtocolSmb

가 Amazon FSx for NetApp ONTAP 파일 시스템의 스토리지 가상 머신(SVM)에 액세스하는 데 AWS DataSync 사용하는 서버 메시지 블록(SMB) 프로토콜 구성을 지정합니다. 자세한 내용은 DataSync에 FSx for ONTAP 파일 서버 액세스 권한 제공을 참조하세요.

내용

CmkSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 DataSync 사용하는 `Password` 또는 자격 증명 세트와 고객 관리형 보안 암호에 대한 구성 정보를 지정합니다 AWS KMS key.

유형: CmkSecretConfig객체

필수 여부: 아니요

CustomSecretConfig

DataSync가 특정 전송 위치에 액세스하는 데 사용하는 `Password` 또는 자격 증명 세트와 같은 고객 관리형 보안 암호의 구성 정보를 지정합니다. 이 구성에는 보안 암호 ARN과 보안 암호에 대한 액세스를 제공하는 IAM 역할의 ARN이 포함됩니다.

유형: CustomSecretConfig객체

필수 여부: 아니요

Domain

스토리지 가상 머신(SVM)이 속한 Windows 도메인의 이름을 지정합니다.

환경에 여러 Active Directory 도메인이 있는 경우 이 파라미터를 구성하면 DataSync가 올바른 SVM에 연결되도록 할 수 있습니다.

유형: 문자열

길이 제약: 최대 길이는 253입니다.

패턴: `^([A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252})?$`

필수 여부: 아니요

MountOptions

가 SMB 파일 서버에 액세스하는 데 AWS DataSync 사용하는 SMB(Server Message Block) 프로토콜의 버전을 지정합니다.

유형: SmbMountOptions객체

필수 여부: 아니요

Password

SVM에 액세스할 수 있는 권한이 있는 사용자의 암호를 지정합니다.

타입: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^.{0,104}$`

필수 여부: 아니요

User

SVM에 파일, 폴더 및 메타데이터를 탑재하고 이에 액세스할 수 있는 사용자를 지정합니다.

전송에 적합한 수준의 액세스 권한을 가진 사용자를 선택하는 방법에 대한 자세한 내용은 SMB 프로토콜 사용을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 104입니다.

패턴: `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

HdfsNameNode

Hadoop 분산 파일 시스템(HDFS)의 NameNode입니다. NameNode는 파일 시스템의 네임스페이스를 관리합니다. NameNode는 파일 및 디렉터리 열기, 닫기 및 이름 바꾸기와 같은 작업을 수행합니다. NameNode에는 데이터 블록을 DataNode에 매핑하기 위한 정보가 들어 있습니다.

내용

Hostname

HDFS 클러스터에 있는 NameNode의 호스트 이름입니다. 이 값은 NameNode의 IP 주소 또는 도메인 이름 서비스(DNS) 이름입니다. 온프레미스에 설치된 에이전트는 이 호스트 이름을 사용하여 네트워크의 NameNode와 통신합니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 255.

패턴: `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9])$`

필수 여부: 예

Port

NameNode가 클라이언트 요청을 수신하는 데 사용하는 포트입니다.

타입: 정수

유효 범위: 최소값 1. 최댓값은 65536입니다.

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LocationFilter

ListLocations에 의해 반환되는 리소스 목록의 범위를 좁히세요. 예컨대, 모든 Amazon S3 위치를 보려면 "Name": "LocationType", "Operator": "Equals"및 "Values": "S3"을 사용하여 필터를 생성하세요.

자세한 설명은 리소스 필터링을 참조하세요.

내용

Name

사용 중인 필터의 이름입니다. 각 API 호출은 사용할 수 있는 필터 목록(예: ListLocations의 경우LocationType) 을 지원합니다.

타입: 문자열

유효 값: LocationUri | LocationType | CreationTime

필수 여부: 예

Operator

필터 값을 비교하는 데 사용되는 연산자(예: Equals또는Contains).

타입: 문자열

유효 값: Equals | NotEquals | In | LessThanOrEqual | LessThan | GreaterThanOrEqual | GreaterThan | Contains | NotContains | BeginsWith

필수 여부: 예

Values

필터링할 값입니다. 예컨대, Amazon S3 위치만 표시할 수 있습니다.

타입: 문자열 배열

길이 제약: 최소 길이 1. 최대 길이는 255.

패턴: ^[0-9a-zA-Z_\ \-\:*\.\\/\?-]*$

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LocationListEntry

위치 목록에 있는 단일 항목을 표시합니다. `LocationListEntry`은 ListLocation 작업이 호출될 때 위치 목록이 포함된 배열을 반환합니다.

내용

LocationArn

해당 위치의 Amazon 리소스 이름(ARN). 네트워크 파일 시스템(NFS) 또는 Amazon EFS의 경우, 위치는 내보내기 경로입니다. Amazon S3의 경우, 위치는 탑재하여 위치의 루트로 사용하려는 접두사 경로입니다.

타입: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

필수 여부: 아니요

LocationUri

위치의 URI 목록을 표시합니다. `LocationUri`ListLocation 작업이 호출될 때 위치 목록이 포함된 배열을 반환합니다.

형식: `TYPE://GLOBAL_ID/SUBDIR`.

TYPE은 위치 타입(예: `nfs`또는`s3`) 을 지정합니다.

GLOBAL_ID는 위치를 뒷받침하는 리소스의 글로벌 고유 식별자입니다. EFS의 한 예는 `us-east-2.fs-abcd1234`입니다. Amazon S3의 예로는 버킷 명칭을 들 수 있습니다(예:`myBucket`). NFS의 예로는 유효한 IPv4, IPv6 주소 또는 DNS를 준수하는 호스트 이름이 있습니다.

SUBDIR은 유효한 파일 시스템 경로로, *nix 규칙과 같이 슬래시로 구분됩니다. NFS 및 Amazon EFS의 경우, 위치를 탑재하기 위한 내보내기 경로입니다. Amazon S3의 경우, 이것은 탑재하여 위치의 루트로 취급하려는 접두사 경로입니다.

타입: 문자열

길이 제약: 최대 길이는 4360입니다.

패턴: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

ManagedSecretConfig

DataSync 관리형 보안 암호의 구성 정보를 지정하며, 여기에는 DataSync가 특정 전송 위치에 액세스하는 데 사용하는 인증 토큰 또는 자격 증명 세트가 포함됩니다. DataSync는 기본 AWS관리형 KMS 키를 사용하여이 보안 암호를 암호화합니다 AWS Secrets Manager.

내용

SecretArn

AWS Secrets Manager 보안 암호의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^(arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

ManifestConfig

AWS DataSync에서 전송하려는 파일 또는 객체 목록인 매니페스트를 구성합니다. 자세한 내용과 구성 예제는 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

내용

Action

DataSync가 매니페스트를 사용하는 대상을 지정합니다.

타입: 문자열

유효 값: `TRANSFER`

필수 여부: 아니요

Format

매니페스트의 파일 형식을 지정합니다. 자세한 내용은 Creating a manifest 섹션을 참조하세요.

타입: 문자열

유효 값: `CSV`

필수 여부: 아니요

Source

DataSync에서 사용할 매니페스트와 호스팅 위치를 지정합니다.

> **Note**
>
> 2024년 2월 7일 이후에 새 매니페스트를 구성하는 경우 이 파라미터를 지정해야 합니다. 그렇지 않으면 DataSync에 대한 IAM 역할이 없어 매니페스트를 호스팅하는 S3 버킷에 액세스할 수 있다는 400 상태 코드와 `ValidationException` 오류가 표시됩니다. 자세한 내용은 Providing DataSync access to your manifest 섹션을 참조하세요.

유형: SourceManifestConfig객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NfsMountOptions

DataSync가 NFS 프로토콜을 사용하여 위치에 액세스하는 방법을 지정합니다.

내용

Version

NFS 공유를 탑재할 때 DataSync에서 사용할 NFS 버전을 지정합니다. 서버가 지정된 버전 사용을 거부하면 태스크가 실패합니다.

다음과 같은 옵션을 지정할 수 있습니다:

- `AUTOMATIC`(기본값): DataSync는 NFS 버전 4.1을 선택합니다.
- `NFS3`: 서버에 비동기 쓰기를 허용하는 상태 비저장 프로토콜 버전입니다.
- `NFSv4_0`: 위임 및 의사 파일 시스템을 지원하는 방화벽 친화적인 상태 저장 프로토콜 버전입니다.
- `NFSv4_1`: 세션, 디렉토리 위임 및 병렬 데이터 처리를 지원하는 상태 저장 프로토콜 버전입니다. NFS 버전 4.1에는 버전 4.0에서 사용할 수 있는 모든 기능이 포함되어 있습니다.

> **Note**
>
> DataSync는 현재 Amazon FSx for NetApp ONTAP 위치에 대해 NFS 버전 3만 지원합니다.

타입: 문자열

유효 값: `AUTOMATIC | NFS3 | NFS4_0 | NFS4_1`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OnPremConfig

NFS(Network File System) 파일 서버에 연결할 수 있는 AWS DataSync 에이전트입니다.

내용

AgentArns

NFS 파일 서버에 연결할 수 있는 DataSync 에이전트의 Amazon 리소스 이름(ARN)입니다.

하나 이상의 에이전트를 지정할 수 있습니다. 자세한 내용은 Using multiple DataSync agents 섹션을 참조하세요.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 8개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

필수 여부: 예

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

Options

전송 작업이 구성된 방식을 나타냅니다. 이러한 옵션에는 DataSync가 전송 중에 파일, 객체 및 관련 메타데이터 처리 방법이 포함됩니다. 또한 다른 옵션 중에서 데이터 무결성을 확인하고, 작업에 대한 대역폭 제한 설정 방법을 지정할 수 있습니다.

각 옵션에는 기본값이 있습니다. 필요한 경우가 아니라면 StartTaskExecution을 호출하기 전에 이러한 옵션을 구성하지 않아도 됩니다.

각 작업 실행에 대해 작업 옵션을 재정의할 수도 있습니다. 예를 들어 개별 실행에 대해 `LogLevel`을 조정할 수 있습니다.

내용

Atime

파일을 마지막으로 읽거나 쓴 시간을 나타내는 메타데이터를 보존할지 여부를 지정합니다.

> **Note**
>
> `Atime`의 동작은 플랫폼 전체에서 완전히 표준이 아니므로 DataSync는 최선의 노력을 다해야 이러한 작업을 수행할 수 있을 뿐입니다.

- `BEST_EFFORT`(기본값) - DataSync는 원본 `Atime` 속성을 모든 소스 파일(즉, 작업 실행의 `PREPARING` 단계 이전 버전)에 보존하려고 시도합니다. 이 옵션이 권장됩니다.
- `NONE` - `Atime`을 무시합니다.

> **Note**
>
> `Atime`이 `BEST_EFFORT`로 설정된 경우 `Mtime`이 `PRESERVE`로 설정되어야 합니다. `Atime`이 `NONE`으로 설정된 경우 `Mtime`도 `NONE`이어야 합니다.

타입: 문자열

유효 값: `NONE | BEST_EFFORT`

필수 여부: 아니요

BytesPerSecond

DataSync 작업에 의해 사용되는 대역폭을 제한합니다. 예를 들어 DataSync에서 최대 1MB를 사용하기를 원하면 이 값을 `1048576(=1024*1024)` 로 설정합니다.

타입: Long

유효한 범위: 최소값은 -1입니다.

필수 여부: 아니요

Gid

파일 소유자의 POSIX 그룹 ID (GID)를 지정합니다.

- `INT_VALUE`(기본값) - 사용자 ID(UID)와 GID의 정수 값을 보존합니다(권장).
- `NONE` - UID와 GID를 무시합니다.

자세한 내용은 Understanding how DataSync handles file and object metadata 섹션을 참조하세요.

타입: 문자열

유효 값: `NONE | INT_VALUE | NAME | BOTH`

필수 여부: 아니요

LogLevel

DataSync가 Amazon CloudWatch Logs 로그 그룹에 게시하는 로그 유형을 지정합니다. 로그 그룹을 지정하려면 CloudWatchLogGroupArn을 참조하세요.

- `BASIC` - 기본 정보(예: 전송 오류)만 포함된 로그를 게시합니다.
- `TRANSFER` - DataSync 작업이 전송하는 모든 파일 또는 객체에 대한 로그를 게시하고 데이터 무결성 검사를 수행합니다.
- `OFF` - 로그가 게시되지 않습니다.

타입: 문자열

유효 값: `OFF | BASIC | TRANSFER`

필수 여부: 아니요

Mtime

작업 실행 `PREPARING` 단계 이전에 파일이 마지막으로 쓰여진 시간을 나타내는 메타데이터의 보존 여부를 지정합니다. 이 옵션은 태스크를 두 번 이상 실행해야 하는 경우에 필요합니다.

- PRESERVE(기본값) - 원래 Mtime을 보존합니다(권장).
- NONE - Mtime을 무시합니다.

> **Note**
>
> Mtime이 PRESERVE로 설정된 경우 Atime이 BEST_EFFORT로 설정되어야 합니다. Mtime이 NONE으로 설정된 경우 Atime도 NONE으로 설정되어야 합니다.

타입: 문자열

유효 값: NONE | PRESERVE

필수 여부: 아니요

ObjectTags

객체 스토리지 시스템 간에 전송할 때 DataSync가 객체 태그(기본 동작)의 PRESERVE 여부를 지정합니다. DataSync 태스크에서 객체 태그를 무시하도록 하려면 NONE 값을 지정합니다.

타입: 문자열

유효 값: PRESERVE | NONE

필수 여부: 아니요

OverwriteMode

DataSync가 대상 위치의 데이터를 수정할지 또는 보존할지 여부를 지정합니다.

- ALWAYS(기본값) - DataSync는 소스 데이터(메타데이터 포함)가 변경될 때 대상 위치의 데이터를 수정합니다.

  DataSync에서 객체를 덮어쓰는 경우, 특정 Amazon S3 스토리지 클래스(예: 검색 또는 조기 삭제)에 대한 추가 요금이 발생할 수 있습니다. 자세한 내용은 Storage class considerations with Amazon S3 transfers 섹션을 참조하세요.
- NEVER - DataSync는 소스 데이터가 변경된 경우에도 대상 위치의 데이터를 덮어쓰지 않습니다. 이 옵션을 사용하여 대상의 파일 또는 객체에 대한 변경 사항을 덮어쓰지 않도록 보호할 수 있습니다.

타입: 문자열

유효 값: ALWAYS | NEVER

필수 여부: 아니요

PosixPermissions

파일의 읽기, 쓰기 또는 실행과 같은 특정 목적을 위해 파일에 액세스할 수 있는 사용자 또는 그룹을 지정하는 값입니다.

자세한 내용은 Understanding how DataSync handles file and object metadata 섹션을 참조하세요.

- PRESERVE(기본값) - POSIX 스타일 권한을 보존합니다(권장).
- NONE - POSIX 스타일 권한을 무시합니다.

> **Note**
>
> DataSync는 소스 위치의 기존 권한을 보존할 수 있습니다.

타입: 문자열

유효 값: NONE | PRESERVE

필수 여부: 아니요

PreserveDeletedFiles

소스 파일 시스템에 존재하지 않는 목적지 장소에 파일을 보존할지 여부를 지정하는 값입니다. 이 옵션은 Amazon S3 스토리지 비용에 영향을 줄 수 있습니다. 작업에서 객체를 삭제하는 경우 특정 스토리지 클래스에 대한 최소 스토리지 기간 요금이 발생할 수 있습니다. 자세한 내용은 DataSync에서 Amazon S3 스토리지 클래스 작업 시 고려 사항을 참조하세요.

- PRESERVE(기본값) - 대상 파일을 무시합니다(권장).
- REMOVE - 소스에 없는 대상 파일을 삭제합니다.

> **Note**
>
> 이 파라미터를 REMOVE로 설정하면, TransferMode를 ALL으로 설정할 수 없습니다. 모든 데이터를 전송할 때 DataSync는 목적지 위치를 스캔하지 않으므로 무엇을 삭제해야 할지 모릅니다.

타입: 문자열

유효 값: PRESERVE | REMOVE

필수 여부: 아니요

PreserveDevices

DataSync가 소스 위치에서 블록 및 문자 장치의 메타데이터를 보존해야 하는지 여부와 목적지에 해당 장치 이름과 메타데이터를 사용하여 파일을 다시 생성해야 하는지 여부를 지정하십시오. DataSync는 이러한 디바이스의 이름과 메타데이터만 복사합니다.

> **Note**
>
> DataSync는 터미널이 아니고 EOF(파일 끝) 마커를 반환하지 않으므로 이러한 장치의 실제 내용을 복사할 수 없습니다.

- NONE(기본값) - 특수 디바이스를 무시합니다(권장).
- PRESERVE - 문자 및 블록 디바이스 메타데이터를 보존합니다. 이 옵션은 현재 Amazon EFS를 위해 지원되지는 않습니다.

타입: 문자열

유효 값: NONE | PRESERVE

필수 여부: 아니요

SecurityDescriptorCopyFlags

소스에서 목적지 객체로 복사로 복사되는 SMB 보안 설명자의 구성 요소를 지정합니다.

이 값은 SMB와 Amazon FSx for Windows File Server 위치 간이나, 두 개의 Windows File Server용 FSx 위치 간의 전송에만 사용됩니다. 자세한 내용은 Understanding how DataSync handles file and object metadata 섹션을 참조하세요.

- OWNER_DACL(기본값) - 복사된 각 객체에 대해 DataSync는 다음 메타데이터를 복사합니다.
  - 객체 소유자
  - 객체에 대한 액세스 권한을 부여할지 여부를 결정하는 NTFS 임의 액세스 제어 목록(DACL)입니다.

    DataSync는 이 옵션을 사용하여 NTFS 시스템 액세스 제어 목록(SACLs)을 복사하지 않습니다.
- OWNER_DACL_SACL - 복사된 각 객체에 대해 DataSync는 다음 메타데이터를 복사합니다.

- 객체 소유자
- 객체에 대한 액세스 권한을 부여할지 여부를 결정하는 NTFS 임의 액세스 제어 목록(DACL)입니다.
- SACL은 관리자가 보안 객체에 액세스하려는 시도를 로깅하는 데 사용됩니다.

  SACL을 복사하려면 DataSync가 SMB 위치에 액세스하는 데 사용하는 Windows 사용자에게 추가 권한을 부여해야 합니다. 올바른 권한을 가진 사용자를 선택하는 방법에 대한 자세한 내용은 SMB, FSx for Windows File Server 또는 FSx for ONTAP에 필요한 권한(전송 시 위치 유형에 따라 다름)을 참조하세요.

- NONE - SMB 보안 설명자 구성 요소는 복사되지 않습니다. 대상 객체는 대상 위치에 액세스하기 위해 제공된 사용자가 소유합니다. DACL 및 SACL은 대상 서버의 구성을 기반으로 설정됩니다.

타입: 문자열

유효 값: `NONE | OWNER_DACL | OWNER_DACL_SACL`

필수 여부: 아니요

TaskQueueing

여러 작업을 실행할 때의 특정 시나리오 동안에 전송 작업을 대기열에 넣을지 여부를 지정합니다. 기본 값은 `ENABLED`입니다.

타입: 문자열

유효 값: `ENABLED | DISABLED`

필수 여부: 아니요

TransferMode

DataSync가 초기 복사 후 위치 간에 달라진 데이터(메타데이터 포함)만 전송할지 아니면 작업을 실행할 때마다 모든 데이터를 전송할지 지정합니다. 반복 전송을 계획한다면 이전 작업 실행 이후 변경된 내용만 전송하는 것이 좋을 수 있습니다.

- `CHANGED`(기본값) - 최초 전체 전송 후 DataSync는 소스 위치와 대상 위치 간에 서로 다른 데이터와 메타데이터만 복사합니다.
- `ALL` - DataSync는 위치 간의 차이를 비교하지 않고 소스의 모든 데이터를 대상으로 복사합니다.

타입: 문자열

유효 값: `CHANGED | ALL`

필수 여부: 아니요

Uid

파일 소유자의 POSIX 사용자 ID (UID)를 지정합니다.

- INT_VALUE(기본값) - UID와 그룹 ID(GID)의 정수 값을 보존합니다(권장).
- NONE - UID와 GID를 무시합니다.

자세한 내용은 DataSync에서 복사한 메타데이터를 참조하세요.

타입: 문자열

유효 값: NONE | INT_VALUE | NAME | BOTH

필수 여부: 아니요

VerifyMode

전송이 완료된 후 DataSync의 데이터 무결성 검사 여부와 검사 방식을 지정합니다.

- ONLY_FILES_TRANSFERRED(권장) - DataSync는 소스 위치에서 전송된 데이터(메타데이터 포함)의 체크섬을 계산합니다. 전송이 완료된 후 DataSync는 이 체크섬을 대상 위치에서 해당 데이터에 대해 계산한 체크섬과 비교합니다.

  > **Note**
  >
  > 확장 모드 작업의 기본 옵션입니다.

  S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스로 전송하는 경우 이 옵션을 사용하는 것이 좋습니다. 자세한 내용은 Amazon S3 위치의 스토리지 클래스 고려 사항을 참조하세요.
- POINT_IN_TIME_CONSISTENT - 전송 종료 시 DataSync는 전체 소스와 대상을 검사하여 두 위치가 완전히 동기화되었는지 확인합니다.

  > **Note**
  >
  > 이는 기본 모드 작업의 기본 옵션이며 현재 확장 모드 작업에서는 지원하지 않습니다.

  매니페스트를 사용하는 경우 DataSync는 매니페스트에 나열된 항목만 스캔하고 확인합니다.

S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스로 전송하는 경우 이 옵션을 사용할 수 없습니다. 자세한 내용은 Amazon S3 위치의 스토리지 클래스 고려 사항을 참조하세요.

- `NONE` - DataSync는 전송 중에만 데이터 무결성 검사를 수행합니다. 다른 옵션과 달리 전송이 끝날 때 추가 확인은 없습니다.

타입: 문자열

유효 값: `POINT_IN_TIME_CONSISTENT | ONLY_FILES_TRANSFERRED | NONE`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

Platform

AWS DataSync에이전트에 대한 플랫폼 관련 세부 정보(예: 버전 번호)

내용

Version

DataSync 에이전트의 버전입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PrivateLinkConfig

AWS DataSync 에이전트가 Virtual Private Cloud(VPC) 서비스 엔드포인트를 AWS 사용하여에 연결하는 방법을 지정합니다. VPC 엔드포인트를 사용하는 에이전트는 퍼블릭 인터넷을 통해 액세스할 수 없습니다.

내용

PrivateLinkEndpoint

AWS PrivateLink가 제공하는 에이전트가 연결할 VPC 엔드포인트를 지정합니다.

유형: 문자열

길이 제약: 최소 길이는 7입니다. 최대 길이는 15입니다.

패턴: `\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`

필수 여부: 아니요

SecurityGroupArns

사용자 VPC 엔드포인트의 DataSync 액세스를 제공하는 보안 그룹의 Amazon 리소스 이름(ARN)을 지정합니다. 하나의 ARN만 지정할 수 있습니다.

유형: 문자열 배열

배열 멤버: 고정된 항목 수는 1개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

필수 여부: 아니요

SubnetArns

VPC 엔드포인트가 위치한 서브넷의 ARN을 지정합니다. 하나의 ARN만 지정할 수 있습니다.

유형: 문자열 배열

배열 멤버: 고정된 항목 수는 1개입니다.

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/subnet-[a-f0-9]+$`

필수 여부: 아니요

VpcEndpointId

에이전트가 연결되는 VPC 엔드포인트의 ID를 지정합니다.

유형: String

패턴: `^vpce-[0-9a-f]{17}$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

QopConfiguration

QOP(Quality of Protection) 구성은 Hadoop 분산 파일 시스템(HDFS) 클러스터에 구성된 원격 프로시저 호출(RPC) 및 데이터 전송 개인 정보 보호 설정을 지정합니다.

내용

DataTransferProtection

HDFS 클러스터에 구성된 데이터 전송 보호 설정입니다. 이 설정은 Hadoop 클러스터의 `hdfs-site.xml` 파일에 있는 `dfs.data.transfer.protection` 설정에 해당합니다.

타입: 문자열

유효 값: `DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY`

필수 여부: 아니요

RpcProtection

HDFS 클러스터에 구성되는 RPC 보호 설정. 이 설정은 Hadoop 클러스터의 `core-site.xml` 파일에 있는 `hadoop.rpc.protection` 설정에 해당합니다.

타입: 문자열

유효 값: `DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportDestination

DataSync가 작업 보고서를 업로드하는 위치를 지정합니다.

내용

S3

DataSync가 작업 보고서를 업로드하는 Amazon S3 버킷을 지정합니다.

유형: ReportDestinationS3객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportDestinationS3

DataSync가 작업 보고서를 업로드하는 Amazon S3 버킷을 지정합니다.

내용

BucketAccessRoleArn

DataSync가 S3 버킷에 작업 보고서를 업로드할 수 있도록 허용하는 IAM 정책의 Amazon 리소스 이름(ARN)을 지정합니다. 자세한 내용은 DataSync가 Amazon S3 버킷에 작업 보고서를 업로드하도록 허용을 참조하세요.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

필수 여부: 예

S3BucketArn

DataSync가 보고서를 업로드하는 S3 버킷의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 268입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

필수 여부: 예

Subdirectory

보고서의 버킷 접두사를 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

ReportOverride

DataSync 작업 보고서의 특정 측면에 대한 세부 수준을 지정합니다.

내용

ReportLevel

작업 보고서에 오류만 포함할지 아니면 성공과 오류를 포함할지를 지정합니다.

예를 들어, 보고서에는 대부분 전송에서 잘 진행되지 않은 내용만 포함될 수 있습니다 (ERRORS_ONLY). 동시에 작업 필터가 제대로 작동하는지도 확인하려고 합니다. 이 경우 DataSync가 성공적으로 건너뛰었던 파일 목록과 전송하지 않은 파일이 전송되었는지를 확인할 수 있습니다 (SUCCESSES_AND_ERRORS).

타입: 문자열

유효 값: `ERRORS_ONLY | SUCCESSES_AND_ERRORS`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportOverrides

DataSync 작업 보고서의 각 측면에 포함된 세부 수준입니다.

내용

Deleted

DataSync가 대상 위치에서 삭제를 시도한 파일, 객체 및 디렉터리에 대한 보고 수준을 지정합니다. 이는 소스에 없는 대상의 데이터를 삭제하도록 작업을 구성한 경우에만 적용됩니다.

유형: ReportOverride객체

필수 여부: 아니요

Skipped

DataSync가 전송 중에 건너뛰려고 시도한 파일, 개체 및 디렉터리에 대한 보고 수준을 지정합니다.

유형: ReportOverride객체

필수 여부: 아니요

Transferred

DataSync가 전송을 시도한 파일, 개체 및 디렉터리에 대한 보고 수준을 지정합니다.

유형: ReportOverride객체

필수 여부: 아니요

Verified

전송 종료 시 DataSync가 확인을 시도한 파일, 객체 및 디렉터리에 대한 보고 수준을 지정합니다.

유형: ReportOverride객체

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportResult

DataSync가 전송을 위한 전체 작업 보고서를 생성했는지 여부를 표시합니다.

내용

ErrorCode

DataSync가 전체 보고서를 생성할 수 없는 경우, 오류와 관련된 코드를 표시합니다.

타입: 문자열

필수 여부: 아니요

ErrorDetail

보고서 생성 문제에 대한 세부 정보를 제공합니다.

타입: 문자열

필수 여부: 아니요

Status

DataSync가 보고서를 계속 작성 중인지, 보고서를 만들었는지, 전체 보고서를 생성할 수 없는지 여부를 표시합니다.

타입: 문자열

유효 값: `PENDING | SUCCESS | ERROR`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3Config

DataSync가 S3 버킷에 액세스하는 데 사용하는 (IAM) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (ARN)을 지정합니다.

자세한 내용은 DataSync에 S3 버킷 액세스 권한 제공을 참조하세요.

내용

BucketAccessRoleArn

DataSync가 S3 버킷에 액세스하는 데 사용하는 IAM 역할의 ARN을 지정합니다.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

필수 여부: 예

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

S3ManifestConfig

사용할 매니페스트를 호스팅할 S3 버킷 AWS DataSync 을 지정합니다. 자세한 내용과 구성 예제는 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

내용

BucketAccessRoleArn

DataSync가 매니페스트에 액세스할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할을 지정합니다. 자세한 내용은 Providing DataSync access to your manifest 섹션을 참조하세요.

유형: 문자열

길이 제약: 최대 길이 2048.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

필수 여부: 예

ManifestObjectPath

매니페스트의 Amazon S3 객체 키를 지정합니다. 여기에는 접두사(예: `prefix/my-manifest.csv`)가 포함될 수 있습니다.

유형: 문자열

길이 제약: 최대 길이는 4096입니다.

패턴: `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

필수 여부: 예

S3BucketArn

매니페스트를 호스팅하는 S3 버킷의 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약: 최대 길이는 268입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

필수 여부: 예

ManifestObjectVersionId

DataSync에서 사용할 매니페스트의 객체 버전 ID를 지정합니다. 이를 설정하지 않으면 DataSync는 최신 버전의 객체를 사용합니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 100.

패턴: `^.+$`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

SmbMountOptions

AWS DataSync가 SMB 파일 서버에 액세스하는 데 사용하는 서버 메시지 블록(SMB) 프로토콜의 버전을 지정합니다.

내용

Version

기본적으로 DataSync는 SMB 파일 서버와의 협상을 기반으로 SMB 프로토콜 버전을 자동으로 선택합니다. 특정 SMB 버전을 사용하도록 DataSync를 구성할 수도 있지만 DataSync가 SMB 파일 서버와 자동으로 협상하는 데 문제가 있는 경우에만 이렇게 하는 것이 좋습니다.

SMB 버전을 구성하기 위한 옵션은 다음과 같습니다.

- `AUTOMATIC`(기본값): DataSync와 SMB 파일 서버는 2.1과 3.1.1 사이에서 상호 지원하는 SMB의 최상위 버전을 협상합니다.

  이는 권장되는 옵션입니다. 대신 파일 서버에서 지원하지 않는 특정 버전을 선택하면 `Operation Not Supported` 오류가 발생할 수 있습니다.
- `SMB3`: 프로토콜 협상을 SMB 버전 3.0.2로만 제한합니다.
- `SMB2`: 프로토콜 협상을 SMB 버전 2.1로만 제한합니다.
- `SMB2_0`: 프로토콜 협상을 SMB 버전 2.0으로만 제한합니다.
- `SMB1`: 프로토콜 협상을 SMB 버전 1.0으로만 제한합니다.

> **Note**
>
> Amazon FSx for NetApp ONTAP 위치를 생성할 때는 `SMB1`옵션을 사용할 수 없습니다.

타입: 문자열

유효 값: `AUTOMATIC | SMB2 | SMB3 | SMB1 | SMB2_0`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SourceManifestConfig

AWS DataSync에서 사용할 매니페스트와 호스팅 위치를 지정합니다. 자세한 내용과 구성 예제는 Specifying what DataSync transfers by using a manifest 섹션을 참조하세요.

내용

S3

매니페스트를 호스팅하는 S3 버킷을 지정합니다.

타입: S3ManifestConfig객체

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TagListEntry

AWS 리소스에 적용된 단일 태그를 나타내는 키-값 페어입니다.

내용

Key

AWS리소스 태그의 키입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:/-]+$`

필수 여부: 예

Value

AWS리소스 태그의 값입니다.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TaskExecutionFilesFailedDetail

작업 실행 중에 DataSync가 준비, 전송, 확인 및 삭제하지 못하는 파일 또는 객체 수입니다.

> **Note**
> 확장 모드 작업에만 적용됩니다.

내용

Delete

작업 실행 중에 DataSync가 삭제하지 못하는 파일 또는 객체의 수입니다.

유형: Long

필수 여부: 아니요

Prepare

작업 실행 중에 DataSync가 준비하지 못하는 파일 또는 객체의 수입니다.

유형: Long

필수 여부: 아니요

Transfer

작업 실행 중에 DataSync가 전송하지 못하는 파일 또는 객체의 수입니다.

유형: Long

필수 여부: 아니요

Verify

작업 실행 중에 DataSync가 확인하지 못한 파일 또는 객체의 수입니다.

유형: Long

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

TaskExecutionFilesListedDetail

DataSync가 사용자 위치에서 찾는 파일 또는 객체의 수입니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

내용

AtDestinationForDelete

DataSync가 대상 위치에서 찾는 파일 또는 객체의 수입니다. 이 카운터는 대상에서 소스에 없는 데이터를 삭제하도록 작업을 구성한 경우에만 적용됩니다.

유형: Long

필수 여부: 아니요

AtSource

DataSync가 소스 위치에서 찾는 파일 또는 객체의 수입니다.

- 매니페스트를 사용하면 DataSync는 매니페스트에 있는 항목(소스 위치의 모든 항목 아님)만 나열합니다.
- 포함 필터를 사용하면 DataSync는 소스 위치에서 필터와 일치하는 항목만 나열합니다.
- 제외 필터를 사용하면 DataSync는 필터를 적용하기 전에 소스 위치에 있는 모든 항목을 나열합니다.

유형: Long

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK

- AWS SDK for Ruby V3

TaskExecutionFoldersFailedDetail

DataSync가 작업 실행 중에 나열, 준비, 전송, 확인 및 삭제하지 못하는 디렉터리 수입니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

내용

Delete

작업 실행 중에 DataSync가 삭제하지 못하는 디렉터리 수입니다.

유형: Long

필수 여부: 아니요

List

작업 실행 중에 DataSync가 나열하지 못하는 디렉터리 수입니다.

유형: Long

필수 여부: 아니요

Prepare

작업 실행 중에 DataSync가 준비하지 못하는 디렉터리 수입니다.

유형: Long

필수 여부: 아니요

Transfer

작업 실행 중에 DataSync가 전송하지 못하는 디렉터리 수입니다.

유형: Long

필수 여부: 아니요

Verify

작업 실행 중에 DataSync가 확인하지 못한 디렉터리 수입니다.

유형: Long

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

TaskExecutionFoldersListedDetail

DataSync가 사용자 위치에서 찾는 디렉터리 수입니다.

> **Note**
>
> 확장 모드 작업에만 적용됩니다.

내용

AtDestinationForDelete

DataSync가 대상 위치에서 찾는 디렉터리 수입니다. 이 카운터는 대상에서 소스에 없는 데이터를 삭제하도록 작업을 구성한 경우에만 적용됩니다.

유형: Long

필수 여부: 아니요

AtSource

DataSync가 소스 위치에서 찾는 디렉터리 수입니다.

- 매니페스트를 사용하면 DataSync는 매니페스트에 있는 항목(소스 위치의 모든 항목 아님)만 나열합니다.
- 포함 필터를 사용하면 DataSync는 소스 위치에서 필터와 일치하는 항목만 나열합니다.
- 제외 필터를 사용하면 DataSync는 필터를 적용하기 전에 소스 위치에 있는 모든 항목을 나열합니다.

유형: Long

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK

- AWS SDK for Ruby V3

TaskExecutionListEntry

ListTaskExecutions 작업과 함께 반환되는 AWS DataSync 작업 실행 목록의 단일 항목을 나타냅니다.

내용

Status

작업의 실행 상태. 자세한 내용은 작업 실행 상태를 참조하십시오.

타입: 문자열

유효 값: `QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR`

필수 여부: 아니요

TaskExecutionArn

작업 실행의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

필수 여부: 아니요

TaskMode

사용 중인 작업 모드입니다. 자세한 내용은 데이터 전송을 위한 작업 모드 선택을 참조하세요.

타입: 문자열

유효 값: `BASIC | ENHANCED`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

TaskExecutionResultDetail

AWS DataSync 작업 실행 결과에 대한 자세한 정보를 제공합니다.

내용

ErrorCode

작업 실행 동안 DataSync에서 발생한 오류입니다. 이 정보를 사용하면 문제 해결에 도움이 됩니다.

유형: 문자열

필수 여부: 아니요

ErrorDetail

작업을 실행하는 동안 DataSync에서 발생한 오류에 대한 자세한 설명입니다. 이 정보를 사용하면 문제 해결에 도움이 됩니다.

유형: 문자열

필수 여부: 아니요

PrepareDuration

작업 실행이 PREPARING 단계에 있었던 시간(밀리초 단위)입니다. 자세한 내용은 작업 실행 상태를 참조하십시오.

확장 모드 작업의 경우 값은 항상 0입니다. 자세한 내용은 DataSync가 데이터 전송을 준비하는 방법을 참조하세요.

타입: Long

유효 범위: 최소값은 0입니다.

필수 여부: 아니요

PrepareStatus

작업 실행에서 PREPARING 단계의 상태입니다. 자세한 내용은 작업 실행 상태를 참조하십시오.

타입: 문자열

유효 값: PENDING | SUCCESS | ERROR

필수 여부: 아니요

TotalDuration

작업 실행이 실행된 시간(밀리초 단위)입니다.

타입: Long

유효 범위: 최소값은 0입니다.

필수 여부: 아니요

TransferDuration

작업 실행이 TRANSFERRING 단계에 있었던 시간(밀리초 단위)입니다. 자세한 내용은 작업 실행 상태를 참조하십시오.

확장 모드 작업의 경우 값은 항상 0입니다. 자세한 내용은 DataSync가 데이터를 전송하는 방법을 참조하세요.

타입: Long

유효 범위: 최소값은 0입니다.

필수 여부: 아니요

TransferStatus

작업 실행에서 TRANSFERRING 단계의 상태입니다. 자세한 내용은 작업 실행 상태를 참조하십시오.

타입: 문자열

유효 값: PENDING | SUCCESS | ERROR

필수 여부: 아니요

VerifyDuration

작업 실행이 VERIFYING 단계에 있었던 시간(밀리초 단위)입니다. 자세한 내용은 작업 실행 상태를 참조하십시오.

확장 모드 작업의 경우 값은 항상 0입니다. 자세한 내용은 DataSync가 데이터의 무결성을 확인하는 방법을 참조하세요.

타입: Long

유효 범위: 최소값은 0입니다.

필수 여부: 아니요

VerifyStatus

작업 실행에서 VERIFYING 단계의 상태입니다. 자세한 내용은 작업 실행 상태를 참조하십시오.

타입: 문자열

유효 값: PENDING | SUCCESS | ERROR

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TaskFilter

API 필터를 사용하여(ListTasks이)가 반환한 리소스 목록의 범위를 좁힐 수 있습니다. 예를 들어 소스 위치의 모든 작업을 검색하려면 필터 이름(LocationId와)과 해당 위치의 ARN(Operator Equals을)를(ListTasks와)과 함께 사용할 수 있습니다.

자세한 내용은 DataSync 리소스 필터링을 참조하세요.

내용

Name

사용 중인 필터의 이름입니다. 각 API 직접 호출은 해당 호출에 사용할 수 있는 필터 목록을 지원합니다. 예를 들어 LocationId의 경우 ListTasks입니다.

타입: 문자열

유효 값: LocationId | CreationTime

필수 여부: 예

Operator

필터 값을 비교하는 데 사용되는 연산자(예: Equals또는Contains).

타입: 문자열

유효 값: Equals | NotEquals | In | LessThanOrEqual | LessThan | GreaterThanOrEqual | GreaterThan | Contains | NotContains | BeginsWith

필수 여부: 예

Values

필터링할 값입니다. 예를 들어 특정 대상 위치의 작업만 표시하기를 원할 수 있습니다.

유형: 문자열 배열

길이 제약: 최소 길이 1. 최대 길이는 255.

패턴: ^[0-9a-zA-Z_\ \-\:*\.\\/\?-]*$

필수 여부: 예

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TaskListEntry

작업 목록에 있는 단일 항목을 나타냅니다. `TaskListEntry`은 ListTasks 작업이 직접 호출되면 작업 목록이 포함된 배열을 반환합니다. 작업에는 동기화할 소스 및 대상 파일 시스템과 작업에 사용할 옵션이 포함됩니다.

내용

Name

태스크의 이름입니다.

유형: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

패턴: `^[a-zA-Z0-9\s+=._:@/-]+$`

필수 여부: 아니요

Status

작업의 상태입니다.

타입: 문자열

유효 값: `AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE`

필수 여부: 아니요

TaskArn

작업의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약: 최대 길이는 128입니다.

패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-eusc|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:task/task-[0-9a-f]{17}$`

필수 여부: 아니요

TaskMode

사용 중인 작업 모드입니다. 자세한 내용은 데이터 전송을 위한 작업 모드 선택을 참조하세요.

타입: 문자열

유효 값: `BASIC | ENHANCED`

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

TaskReportConfig

사용자 AWS DataSync전송에 대한 세부 정보를 제공하는 작업 보고서 구성 방법을 지정합니다.

자세한 내용은 작럽 보고서 단원을 참조하십시오.

내용

Destination

DataSync가 작업 보고서를 업로드하는 Amazon S3 버킷을 지정합니다. 자세한 내용은 작업 보고서 단원을 참조하십시오.

유형: ReportDestination객체

필수 여부: 아니요

ObjectVersionIds

작업 보고서에 S3 버킷으로 전송된 각 객체의 새 버전 포함 여부를 지정합니다. 이는 버킷의 버전 관리를 활성화한 경우에만 적용됩니다. 이 값을 INCLUDE로 설정하면 작업 실행 기간이 늘어날 수 있다는 점에 유의하세요.

타입: 문자열

유효 값: INCLUDE | NONE

필수 여부: 아니요

OutputType

원하는 작업 보고서 유형을 지정합니다.

- SUMMARY_ONLY: 전송된 파일, 개체, 디렉터리 수, 전송 기간 등 작업에 필요한 세부 정보를 제공합니다.
- STANDARD: 전송, 건너뛰기, 확인된 파일, 개체 및 디렉터리의 전체 목록을 포함하여 작업에 대한 전체 세부 정보를 제공합니다.

타입: 문자열

유효 값: SUMMARY_ONLY | STANDARD

필수 여부: 아니요

Overrides

작업 보고서 측면에 대한 보고 수준을 사용자 지정합니다. 예를 들어 보고서에는 일반적으로 오류만 포함될 수 있지만 DataSync가 대상 위치에서 삭제를 시도한 파일에 대해서만 성공 및 오류 목록을 표시하도록 지정할 수 있습니다.

유형: ReportOverrides객체

필수 여부: 아니요

ReportLevel

작업 보고서에 전송 문제가 발생한 부분만 포함할지 아니면 성공 및 실패 항목의 목록만 포함할지를 지정합니다.

- ERRORS_ONLY: 보고서에는 DataSync가 전송, 건너뛰기, 확인 및 삭제하지 못한 항목이 표시됩니다.
- SUCCESSES_AND_ERRORS: 보고서에는 DataSync가 전송, 건너뛰기, 확인 및 삭제할 수 있었던 항목과 할 수 없었던 항목이 표시됩니다.

타입: 문자열

유효 값: ERRORS_ONLY | SUCCESSES_AND_ERRORS

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TaskSchedule

일정(최소 1시간 간격)에 따라 실행되도록 AWS DataSync 작업을 구성합니다.

내용

ScheduleExpression

Cron 및 Rate 표현식을 사용하여 작업 일정을 지정합니다.

특정 시간 및 날짜에 실행되는 작업 일정에 Cron 표현식을 사용합니다. 예를 들어 다음 Cron 표현식은 매월 첫 번째 수요일 오전 8시에 실행되는 작업 일정을 생성합니다.

```
cron(0 8 * * 3#1)
```

정기적으로 실행되는 작업 일정에 Rate 표현식을 사용합니다. 예를 들어 다음 Rate 표현식은 12시간마다 실행되는 작업 일정을 생성합니다.

```
rate(12 hours)
```

Cron 표현식 및 Rate 표현식 구문에 대한 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

유형: 문자열

길이 제약: 최대 길이 256.

패턴: `^[a-zA-Z0-9\ \_\*\?\,\|\^\-\/\#\s\(\)\+]*$`

필수 여부: 예

Status

작업 일정을 활성화할지 아니면 비활성화할지 지정합니다. 일정은 기본적으로 활성화되어 있지만 비활성화해야 하는 상황이 있을 수 있습니다. 예를 들어 작업 문제를 해결하거나 스토리지 시스템에서 유지 관리를 수행하려면 반복 전송을 일시 중지해야 할 수 있습니다.

동일한 오류로 작업이 반복적으로 실패하면 DataSync가 일정을 자동으로 비활성화할 수 있습니다. 자세한 내용은 TaskScheduleDetails 섹션을 참조하세요.

타입: 문자열

유효 값: `ENABLED | DISABLED`

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TaskScheduleDetails

AWS DataSync 작업 일정에 대한 정보를 제공합니다.

내용

DisabledBy

작업 일정이 비활성화된 방식을 나타냅니다.

- USER - UpdateTask 작업 또는 DataSync 콘솔을 사용하여 일정을 수동으로 비활성화했습니다.
- SERVICE - 동일한 오류로 작업이 반복적으로 실패했기 때문에 DataSync에서 일정을 자동으로 비활성화했습니다.

타입: 문자열

유효 값: `USER | SERVICE`

필수 여부: 아니요

DisabledReason

작업 일정이 비활성화된 경우 이유를 제공합니다.

USER에서 일정을 비활성화하면 `Manually disabled by user.` 메시지가 표시됩니다.

SERVICE에서 일정을 비활성화하면 작업이 계속 실패하는 이유를 이해하는 데 도움이 되는 오류 메시지가 표시됩니다. DataSync 오류 해결에 대한 자세한 내용은 Troubleshooting issues with DataSync transfers 섹션을 참조하세요.

유형: 문자열

길이 제약: 최대 길이는 8192입니다.

패턴: `^[\w\s.,'?!:;\/=|<>()-]*$`

필수 여부: 아니요

StatusUpdateTime

작업 일정의 상태가 마지막으로 변경된 시간을 나타냅니다. 예를 들어 반복되는 오류로 인해 DataSync가 자동으로 일정을 비활성화하는 경우 일정이 비활성화된 시기를 확인할 수 있습니다.

유형: 타임스탬프

필수 여부: 아니요

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

일반적인 오류 유형

이 섹션에는이 AWS 서비스가 반환할 수 있는 일반적인 오류 유형이 나열되어 있습니다. 모든 서비스가 여기에 나열된 모든 오류 유형을 반환하는 것은 아닙니다. 이 서비스의 API 작업에 대한 오류는 해당 API 작업에 대한 주제를 참조하세요.

AccessDeniedException

이 작업을 수행하려면 권한이 있어야 합니다. IAM 정책에 필요한 권한이 포함되어 있는지 확인합니다.

HTTP 상태 코드: 403

ExpiredTokenException

요청에 포함된 보안 토큰이 만료되었습니다. 새 보안 토큰을 요청하고 다시 시도하세요.

HTTP 상태 코드: 403

IncompleteSignature

요청 서명이 AWS 표준을 준수하지 않습니다. 유효한 AWS 자격 증명을 사용하고 있고 요청의 형식이 올바른지 확인합니다. SDK를 사용하는 경우 최신 상태인지 확인합니다.

HTTP 상태 코드: 403

InternalFailure

내부 서버 문제로 인해 현재 요청을 처리할 수 없습니다. 나중에 다시 시도해 주세요. 문제가 지속되면 AWS Support에 문의하십시오.

HTTP 상태 코드: 500

MalformedHttpRequestException

요청 본문을 처리할 수 없습니다. 이는 일반적으로 지정된 콘텐츠 인코딩 알고리즘을 사용하여 요청 본문의 압축을 풀 수 없는 경우에 발생합니다. 콘텐츠 인코딩 헤더가 사용된 압축 형식과 일치하는지 확인합니다.

HTTP 상태 코드: 400

NotAuthorized

이 작업을 수행할 권한이 없습니다. IAM 정책에 필요한 권한이 포함되어 있는지 확인합니다.

HTTP 상태 코드: 401

OptInRequired

AWS 계정에이 서비스에 대한 구독이 필요합니다. 계정에서 서비스를 활성화했는지 확인합니다.

HTTP 상태 코드: 403

RequestAbortedException

응답이 반환되기 전에 요청이 중단되었습니다. 이는 일반적으로 클라이언트가 연결을 닫을 때 발생합니다.

HTTP 상태 코드: 400

RequestEntityTooLargeException

요청 엔티티가 너무 큽니다. 요청 본문의 크기를 줄이고 다시 시도하세요.

HTTP 상태 코드: 413

RequestTimeoutException

요청 시간이 초과되었습니다. 서버가 예상 기간 내에 전체 요청을 받지 못했습니다. 다시 시도하세요.

HTTP 상태 코드: 408

ServiceUnavailable

서비스를 일시적으로 사용할 수 없습니다. 나중에 다시 시도해 주세요.

HTTP 상태 코드: 503

ThrottlingException

요청 속도가 너무 높습니다. AWS SDKs 자동으로 재시도합니다. 요청 횟수를 줄입니다.

HTTP 상태 코드: 400

UnknownOperationException

작업 또는 작업이 인식되지 않습니다. 작업 이름의 철자가 올바르고 사용 중인 API 버전에서 지원되는지 확인합니다.

HTTP 상태 코드: 404

UnrecognizedClientException

제공한 X.509 인증서 또는 AWS 액세스 키 ID가 레코드에 없습니다. 유효한 자격 증명을 사용하고 있고 만료되지 않았는지 확인합니다.

HTTP 상태 코드: 403

ValidationError

입력이 필수 형식 또는 제약 조건을 충족하지 않습니다. 모든 필수 파라미터가 포함되어 있고 값이 유효한지 확인합니다.

HTTP 상태 코드: 400

공통 파라미터

다음 목록에는 모든 작업이 쿼리 문자열을 사용하여 Signature Version 4 요청에 서명하는 데 사용하는 파라미터가 포함되어 있습니다. 작업별 파라미터는 그 작업에 대한 항목에 나열되어 있습니다. 서명 버전 4에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하세요.

X-Amz-Algorithm

요청 서명을 생성하는 데 사용된 해시 알고리즘입니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

타입: 문자열

유효 값: `AWS4-HMAC-SHA256`

필수 항목 여부: 조건부

X-Amz-Credential

자격 증명 범위 값이며 액세스 키, 날짜, 대상으로 하는 리전, 요청하는 서비스 및 종료 문자열("aws4_request")이 포함된 문자열입니다. 값은 다음 형식으로 표시됩니다. access_key/YYYYMMDD/region/service/aws4_request.

자세한 내용은 IAM 사용 설명서의 서명된 AWS API 요청 생성을 참조하세요.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

타입: 문자열

필수 항목 여부: 조건부

X-Amz-Date

서명을 만드는 데 사용되는 날짜입니다. 형식은 ISO 8601 기본 형식(YYYYMMDD'T'HHMMSS'Z')이어야 합니다. 예를 들어 다음 날짜 시간은 유효한 X-Amz-Date 값: `20120325T120000Z`.

조건: X-Amz-Date는 모든 요청에서 옵션이지만 서명 요청에 사용되는 날짜보다 우선할 때 사용됩니다. 날짜 헤더가 ISO 8601 기본 형식으로 지정된 경우 X-Amz-Date가 필요하지 않습니다. X-Amz-Date를 사용하는 경우 항상 Date 헤더의 값을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명 요소를 참조하세요.

타입: 문자열

필수 항목 여부: 조건부

X-Amz-Security-Token

AWS Security Token Service ()에 대한 호출을 통해 얻은 임시 보안 토큰입니다AWS STS. AWS STS의 임시 보안 인증 정보를 지원하는 서비스 목록은 IAM 사용 설명서의 IAM으로 작업하는AWS 서비스를 참조하세요.

조건:에서 임시 보안 자격 증명을 사용하는 경우 보안 토큰을 포함해야 AWS STS합니다.

타입: 문자열

필수 항목 여부: 조건부

X-Amz-Signature

서명할 문자열과 파생된 서명 키에서 계산된 16진수로 인코딩된 서명을 지정합니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

타입: 문자열

필수 항목 여부: 조건부

X-Amz-SignedHeaders

표준 요청의 일부로 포함된 모든 HTTP 헤더를 지정합니다. 서명된 헤더 지정에 대한 자세한 내용은 IAM 사용 설명서의 서명된 AWS API 요청 생성을 참조하세요.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

타입: 문자열

필수 항목 여부: 조건부

문서 이력

다음 표에서는 AWS DataSync 설명서에 추가된 중요 사항에 대해 설명합니다. 당사는 사용자의 피드백을 적용하기 위해 설명서를 자주 업데이트 합니다.

이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하세요.

변경 사항	설명	날짜
VPC 엔드포인트 정책 및 FIPS 지원 VPC 엔드포인트에 대한 지원 추가	이제 VPC 엔드포인트 정책을 사용하고 FIPS 지원 AWS 리전에서 FIPS VPC 엔드포인트를 선택할 수 있습니다.	2025년 9월 30일
IPv6 주소에 대한 지원 추가	이제 IPv4 및 IPv6 주소를 사용하여 DataSync에 연결하고 지원되는 데이터 소스를 사용하여 데이터를 전송할 수 있습니다.	2025년 7월 16일
Discovery 지원 중단	2025년 5월 20일부터 Discovery는 DataSync 기능을 더는 지원하지 않습니다.	2025년 5월 20일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	이 `AWSDataSyncFullAccess` 정책은 DataSync가 Secrets Manager 보안 암호 생성 시 사용하는 권한에서 태그 지정 조건을 제거하는 권한 문 업데이트를 포함합니다.	2025년 5월 13일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	`AWSDataSyncFullAccess` 정책에는 DataSync가 작업할 수 있는 새로운 권한이 있습니다 AWS Secrets Manager.	2025년 5월 7일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	`AWSDataSyncFullAccess` 정책에는 DataSync가 작	2025년 4월 23일

	업할 수 있는 새로운 권한이 있습니다 AWS Secrets Manager.	
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	`AWSDataSyncFullAccess` 정책에는 DataSync가 AWS Secrets Manager 및와 함께 작동하도록 허용하는 새로운 권한이 있습니다 AWS Key Management Service.	2025년 4월 23일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	`AWSDataSyncServiceRolePolicy` 에는 DataSync가 작업할 수 있는 새로운 권한이 있습니다 AWS Secrets Manager.	2025년 4월 15일
대규모 데이터 마이그레이션 수행	온프레미스 또는 기타 클라우드 스토리지에서 AWS로 파일 또는 객체를 전송하기 위해 DataSync를 사용하여 대규모 데이터 마이그레이션을 계획하는 방법을 알아봅니다.	2025년 2월 19일
SMB 위치에서 Kerberos 지원	DataSync는 이제 SMB(Server Message Block) 파일 서버에 연결할 때 Kerberos 인증을 사용할 수 있습니다.	2025년 1월 28일
New AWS 리전	AWS DataSync 는 멕시코(중부) 리전의 데이터 전송에 사용할 수 있습니다.	2025년 1월 14일
New AWS 리전	AWS DataSync 는 아시아 태평양(태국) 리전의 데이터 전송에 사용할 수 있습니다.	2025년 1월 7일

AWS 스토리지 위치 업데이트	이제 Amazon S3, Amazon EFS, Amazon FSx 전송 위치를 업데이트할 수 있습니다.	2024년 12월 18일
Snowball Edge 지원 중단	2024년 11월 12일부터 DataSync는 AWS Snowball Edge을 더는 지원하지 않습니다.	2024년 11월 13일
새로운 AWS 관리형 정책	`AWSServiceRoleForDataSync` 라는 이름의 DataSync 서비스 연결 역할은 `AWSDataSyncServiceRolePolicy` 이라는 새로운 관리형 정책을 사용합니다.	2024년 10월 30일
확장 모드 소개	확장 모드를 사용하면 Amazon S3 위치 간에 사실상 무제한의 객체를 전송할 수 있습니다.	2024년 10월 30일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	이 `AWSDataSyncFullAccess` 정책에는 DataSync로 작동하는 서비스에 대한 새로운 권한이 있습니다.	2024년 10월 30일
Azure 스토리지 범용 v1 계정 지원	DataSync는 Microsoft Azure Blob Storage 간 전송할 때 Azure 스토리지 범용 v1 계정과 함께 작동할 수 있습니다.	2024년 10월 4일
작업 일정을 구성하는 새로운 방법	rate 표현식을 사용하여 DataSync 작업 일정을 구성할 수 있습니다.	2024년 8월 22일
New AWS 리전	AWS DataSync 는 아시아 태평양(말레이시아) 리전의 데이터 전송에 사용할 수 있습니다.	2024년 8월 21일

옵트인 리전이 포함된 에이전트 없는 리전 간 전송 지원	하나 이상의 AWS 스토리지 위치가 옵트인 상태일 때 스토리지 서비스 간 전송에 더 이상 DataSync 에이전트가 필요하지 않습니다 AWS 리전.	2024년 7월 24일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	이 AWSDataSyncFullAccess 정책에는 DataSync로 작동하는 서비스에 대한 새로운 권한이 있습니다.	2024년 7월 22일
S3 교차 계정 자습서 업데이트	이 전송에 더 이상 필요하지 않은 일부 소스 계정의 사용자 권한을 제거했습니다.	2024년 6월 10일
새 작업 실행 상태	CANCELLING 상태는 작업 실행이 취소되는 시기를 나타냅니다.	2024년 5월 15일
작업 일정 일시 중지를 위한 새 옵션	문제를 해결하거나 스토리지 시스템 유지 관리를 수행해야 하는 경우 AWS DataSync 작업 일정을 비활성화할 수 있습니다.	2024년 4월 24일
FIPS 엔드포인트에 대한 TLS 암호 업데이트	AWS DataSync 는 FIPS(Federal Information Processing Standard) 서비스 엔드포인트에 TLS_AES_128_GCM_SHA256(secp256r1) 암호를 사용합니다.	2024년 4월 22일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	이 AWSDataSyncFullAccess 정책에는 DataSync로 작동하는 서비스에 대한 새로운 권한이 있습니다.	2024년 2월 16일

매니페스트를 사용하여 특정 파일 또는 객체 전송	AWS DataSync 는 매니페스트를 사용하여 파일 또는 객체 목록을 전송할 수 있습니다.	2024년 2월 7일
New AWS 리전	AWS DataSync 이제 캐나다 서부(캘거리) 리전에서 데이터를 전송할 수 있습니다.	2023년 12월 20일
추가 클라우드 공급자에 대한 전송 지원	AWS DataSync 는 이제 AWS 스토리지 서비스와 IBM Cloud Object Storage 또는 간에 데이터를 전송할 수 있습니다Seagate Lyve Cloud.	2023년 11월 7일
(Alibaba Cloud Object Storage Service을)를 사용한 전송 지원	AWS DataSync 는 이제 AWS 스토리지 서비스와 간에 데이터를 전송할 수 있습니다 Alibaba Cloud Object Storage Service.	2023년 9월 25일
작업 보고서 지원	작업 보고서를 사용하여 AWS DataSync 전송을 모니터링합니다.	2023년 8월 30일
New AWS 리전	AWS DataSync 이제 이스라엘(텔아비브) 리전에서 데이터를 전송할 수 있습니다.	2023년 8월 23일
추가 클라우드 공급자에 대한 전송 지원	AWS DataSync 는 이제 AWS 스토리지 서비스와 여러 다른 클라우드 공급자(예: Wasabi Cloud Storage, DigitalOcean Spaces및 Oracle Cloud Infrastructure Object Storage) 간에 데이터를 전송할 수 있습니다.	2023년 8월 8일

Microsoft Azure Blob Storage 지원의 일반 가용성	AWS DataSync 는 이제와 객체를 주고받을 수 있습니다Microsoft Azure Blob Storage.	2023년 7월 25일
TLS 1.3 지원	스토리지 위치 간에 전송할 때는 AWS DataSync 이제 TLS(전송 계층 보안) 1.3을 사용하여 모든 네트워크 트래픽을 암호화합니다.	2023년 6월 28일
새로운 DataSync 검색 지표	AWS DataSync Discovery 는 이제 스토리지 리소스 클러스터, 스토리지 가상 머신(SVM) 또는 볼륨에 있는 LUNs(논리적 단위 번호) 수를 알려줄 수 있습니다.	2023년 6월 28일
New AWS 리전	AWS DataSync 이제 아시아 태평양(멜버른) 리전에서 데이터를 전송할 수 있습니다.	2023년 5월 24일
Snowball Edge의 S3 호환 스토리지 지원	AWS DataSync 를 사용하여의 Amazon S3 호환 스토리지 AWS Snowball Edge 와 AWS 스토리지 서비스 간에 데이터를 전송할 수 있습니다.	2023년 5월 18일
AWS 관리형 정책 업데이트 - 기존 정책 업데이트	이 `AWSDataSyncFullAccess` 정책에는 DataSync로 작동하는 서비스에 새로운 권한이 있습니다.	2023년 5월 2일
의 일반 가용성 AWS DataSync Discovery	DataSync Discovery를 사용하여 AWS로의 마이그레이션이 가속화됩니다.	2023년 4월 25일

Microsoft Azure Blob Storage 지원의 공개 프리뷰 릴리스	AWS DataSync 는 이제에서 객체를 전송할 수 있습니다Microsoft Azure Blob Storage.	2023년 3월 29일
새 IAM 정책	DataSync는 DataSync 검색 기능을 지원하기 위해 `AWSServiceRoleForDataSyncDiscovery` 이름의 서비스 연동 역할을 사용합니다.	2023년 3월 21일
New AWS 리전	AWS DataSync 이제 AWS 리전아시아 태평양(하이데라바드), 유럽(스페인), 유럽(취리히)에서를 사용할 수 있습니다.	2023년 2월 6일
작업 실행에 태그 사용	이제 AWS DataSync 작업 실행에 태그를 지정할 수 있습니다.	2022년 12월 16일
S3 Glacier Instant Retrieval 지원	이제 S3 Glacier Instant Retrieval 스토리지 클래스에 직접 객체를 전송할 수 있습니다.	2022년 12월 16일
객체 시스템 메타데이터 복사	AWS DataSync 는 이제 객체 스토리지 시스템과 Amazon S3 간에 전송할 때 시스템 메타데이터를 복사할 수 있습니다.	2022년 12월 16일
New AWS 리전	AWS DataSync 이제 중국(베이징) 및 중국(닝샤) 리전에서를 사용할 수 있습니다.	2022년 12월 14일
New AWS 리전	AWS DataSync 이제 중동(UAE) 리전에서를 사용할 수 있습니다.	2022년 11월 16일

객체 스토리지 위치가 있는 자체 서명 인증서 지원	AWS DataSync 는 자체 서명 또는 프라이빗 인증서를 사용하는 객체 스토리지 위치에 연결할 수 있습니다.	2022년 10월 25일
데이터 압축 정보 가져오기	AWS DataSync 는 압축이 적용된 후 네트워크를 통해 전송된 물리적 바이트 수를 제공할 수 있습니다.	2022년 10월 25일
의 공개 미리 보기 릴리스 AWS DataSync Discovery	DataSync Discovery를 사용하여 AWS로의 마이그레이션이 가속화됩니다.	2022년 9월 21일
Google Cloud Storage 내/외부로 데이터를 마이그레이션하는 새로운 옵션	Google Cloud에 AWS DataSync 에이전트를 배포하여 Google Cloud Storage로 또는 Google Cloud Storage에서 데이터를 전송할 수 있습니다.	2022년 7월 21일
Amazon FSx for NetApp ONTAP 파일 시스템 지원	AWS DataSync 는 이제 FSx for ONTAP 파일 시스템과 파일 및 폴더를 주고 받을 수 있습니다.	2022년 6월 28일
Amazon EFS 위치용 새로운 보안 옵션	AWS DataSync 는 TLS, 액세스 포인트 및 IAM 역할을 사용하여 Amazon EFS 파일 시스템에 액세스할 수 있습니다.	2022년 5월 31일
Google Cloud Storage 및 Azure 파일 내/외부로 데이터를 마이그레이션하기	를 사용하면 Google Cloud Storage 및 Azure 파일 간에 데이터를 전송할 AWS DataSync 수 있습니다. 자세한 내용은 객체 스토리지용 위치 생성 및 SMB에 위치 생성을 참조하세요.	2022년 5월 24일

새 AWS DataSync 작업 설정	객체 태그 복사 옵션을 사용하면 객체 스토리지 시스템 간에 전송할 때 객체 태그 유지 여부를 지정할 수 있습니다.	2022년 5월 5일
New AWS 리전	AWS DataSync 이제 아시아 태평양(자카르타) 리전에서를 사용할 수 있습니다.	2022년 4월 19일
Amazon FSx for OpenZFS 파일 시스템 지원	AWS DataSync 는 이제 FSx for OpenZFS 파일 시스템과 파일 및 폴더를 주고 받을 수 있습니다.	2022년 4월 5일
Amazon FSx for Lustre 파일 시스템 지원	AWS DataSync 는 이제 FSx for Lustre 파일 시스템과 파일 및 폴더를 주고 받을 수 있습니다.	2021년 12월 10일
Hadoop 분산 파일 시스템 (HDFS) 지원	AWS DataSync 는 이제 HDFS 클러스터에서 파일 및 폴더 전송을 지원합니다.	2021년 11월 3일
New AWS 리전	AWS DataSync 이제 아시아 태평양(오사카) 리전에서를 사용할 수 있습니다.	2021년 7월 28일
AWS 스토리지 서비스 간 완전 자동화된 전송	AWS DataSync 이제는 DataSync 콘솔에서 몇 번의 클릭만으로 Amazon S3, Amazon EFS 또는 FSx for Windows File Server 간에 파일 또는 객체를 전송할 수 있습니다.	2020년 11월 9일

실행 중인 작업이 사용하는 네트워크 대역폭 조정	AWS DataSync 이제를 통해 고객은 실행 중인 DataSync 작업에서 사용하는 네트워크 대역폭을 조정할 수 있습니다. 이렇게 하면 작업에 며칠이 걸리는 다른 사용자나 애플리케이션에 미치는 영향을 최소화 할 수 있습니다.	2020년 11월 9일
향상된 온프레미스 DataSync 가상 머신(VM) 기능 지원	AWS DataSync 에이전트 VM 호스트 콘솔은 이제 로컬 콘솔에서 에이전트를 활성화하는 등 향상된 기능을 지원합니다.	2020년 10월 19일
AWS DataSync 이제에서 데이터를 송수신할 수 있습니다. AWS Outposts	DataSync는 이제 AWS Outposts의 Amazon S3 내/외부로 객체 전송을 지원합니다.	2020년 9월 30일
API 필터링 지원	AWS DataSync 는 이제 `ListTasks` 및 `ListLocations` API 호출에 대한 필터링을 지원하므로 데이터 전송을 위한 소스 또는 대상과 같은 필터를 사용하여 데이터 전송 작업의 구성을 쉽게 검색할 수 있습니다.	2020년 8월 18일
자체 관리형 객체 스토리지의 데이터 복사 지원	AWS DataSync 는 이제 자체 관리형 객체 스토리지와 Amazon S3, Amazon Elastic File System 또는 FSx for Windows File Server 간의 데이터 전송을 지원합니다.	2020년 7월 27일

Linux 커널 기반 가상 머신 (KVM) 및 Microsoft Hyper-V 하이퍼바이저 지원	AWS DataSync 는 이제 기존 VMware 및 Amazon EC2 옵션 외에도 KVM 및 Microsoft Hyper-V 가상화 플랫폼에 온프레미스 에이전트를 배포할 수 있는 기능을 제공합니다.	2020년 7월 1일
AWS DataSync 이제에서 Amazon CloudWatch Logs 구성을 자동으로 구성할 수 있습니다.	DataSync를 사용하면 데이터 전송을 위한 로그를 게시하는 데 필요한 CloudWatch 로그 그룹과 리소스 정책을 자동으로 생성할 수 있는 옵션을 가지게 되어 작업 생성 및 모니터링 설정이 간소화됩니다.	2020년 7월 1일
AWS DataSync 이제에서 데이터를 송수신할 수 있습니다. AWS Snowball Edge	이제 DataSync는 엣지 컴퓨팅 및 데이터 전송 디바이스의 가장 AWS Snowball Edge작은 멤버인와 파일을 주고 받을 AWS Snow Family 수 있도록 지원합니다. Snowcone Edge는 휴대가 가능하고, 견고하고, 안전할 뿐 아니라, 배낭에 들어갈 만큼 작고 가벼워 열악한 사용 환경에서도 사용할 수 있습니다.	2020년 6월 17일
New AWS 리전	AWS DataSync 이제 아프리카(케이프타운) 리전과 유럽(밀라노) 리전에서를 사용할 수 있습니다.	2020년 6월 16일

향상된 파일 수준 로깅 모니터링 기능	이제 NFS 서버, SMB 서버, Amazon S3 버킷, Amazon EFS 파일 시스템 및 FSx for Windows File Server 파일 시스템 간에 복사된 파일 및 객체에 자세한 로깅을 활성화할 수 있습니다.	2020년 4월 24일
SMB 공유와 Amazon FSx for Windows File Server 간에 데이터 복사 지원	이제 SMB 공유와 FSx for Windows File Server 간에 데이터를 복사할 수 있습니다.	2020년 1월 24일
작업 예약 지원	이제 작업을 수동으로 실행하거나 지정된 일정에 따라 실행되도록 예약할 수 있습니다.	2019년 11월 20일
New AWS 리전	AWS DataSync 이제 아시아 태평양(홍콩) 리전, 아시아 태평양(뭄바이) 리전, 유럽(스톡홀름) 리전, 남아메리카(상파울루) 리전 및 AWS GovCloud(미국 동부) 리전에서를 사용할 수 있습니다.	2019년 11월 20일
New AWS 리전	AWS DataSync 이제 캐나다(중부) 리전, 유럽(런던) 리전 및 유럽(파리) 리전에서를 사용할 수 있습니다.	2019년 10월 2일
Amazon S3 스토리지 클래스 지원	현재 Amazon S3 스토리지 클래스에 직접 객체를 전송할 수 있습니다.	2019년 9월 24일
New AWS 리전	AWS DataSync 이제 중동(바레인) 리전에서를 사용할 수 있습니다.	2019년 8월 28일

SMB(Server Message Block) 공유와 Amazon S3 또는 Amazon EFS 간에 데이터 복사 지원	이제 SMB 파일 공유와 Amazon S3 또는 Amazon EFS 간에 데이터를 복사할 수 있습니다.	2019년 8월 22일
Virtual Private Cloud(VPC) 엔드포인트 사용 지원	이제 에이전트 AWS 와 간에 프라이빗 연결을 생성하고 프라이빗 네트워크에서 작업을 실행할 수 있습니다. 그러면 네트워크에서 데이터를 복사할 때 데이터 보안이 강화됩니다.	2019년 8월 5일
FIPS(연방 정보 처리 표준) 엔드포인트 지원	이제 FIPS 엔드포인트를 사용하여 에이전트를 만들고 작업을 실행할 수 있습니다.	2019년 8월 5일
New AWS 리전	AWS DataSync 이제를 AWS GovCloud(미국 서부) 리전에서 사용할 수 있습니다.	2019년 6월 11일
필터링 지원	이제 소스 위치에서 대상 위치로 데이터를 전송할 때 필터를 적용하여 소스 위치에 있는 파일의 하위 집합만 전송할 수 있습니다.	2019년 5월 22일
의 첫 번째 릴리스 AWS DataSync	AWS DataSync 서비스의 일반 릴리스입니다.	2018년 11월 26일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하십시오.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.