시작하십시오
Cloud Sync

NetApp
May 02, 2022

목차

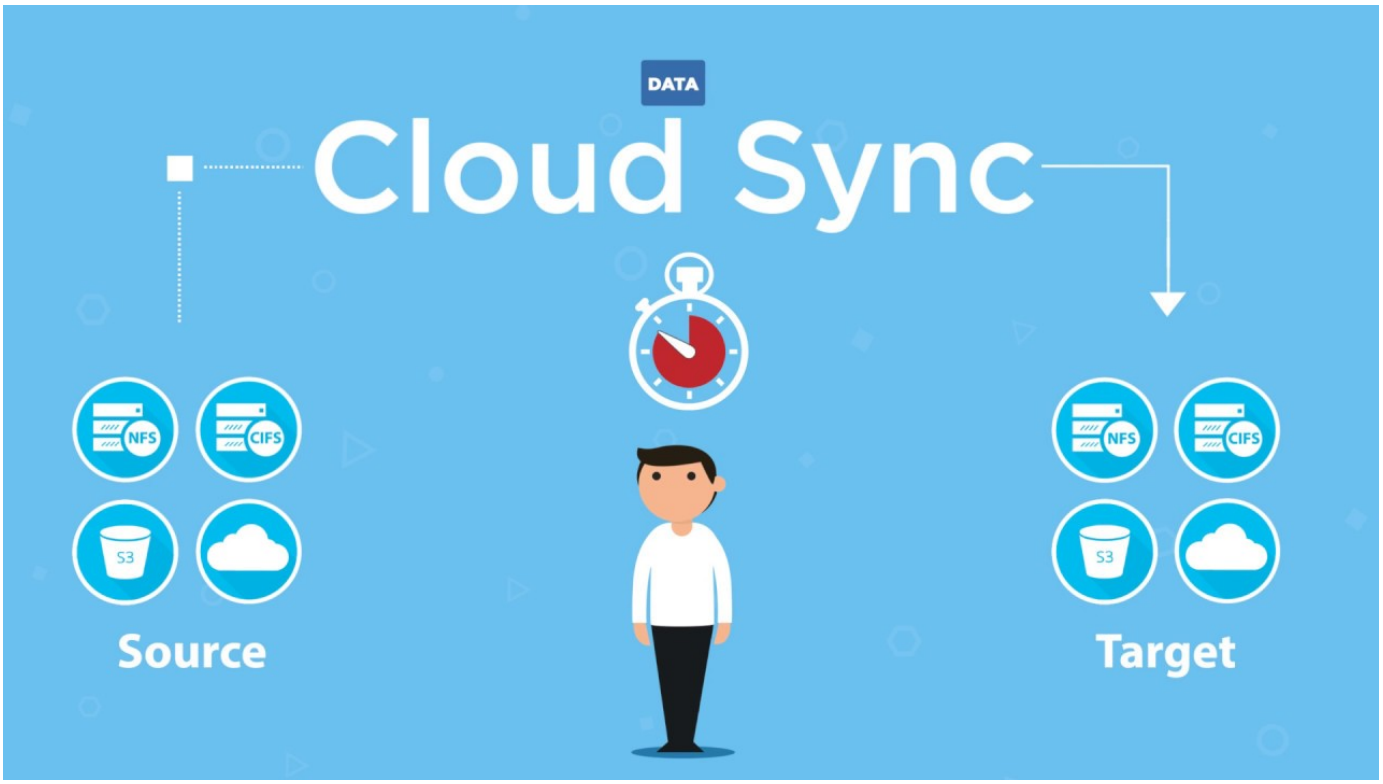
시작하십시오

Cloud Sync 개요

NetApp Cloud Sync 서비스는 데이터를 클라우드 또는 온프레미스의 모든 타겟으로 간단하고 안전하며 자동화된 방법으로 마이그레이션합니다. StorageGRID는 파일 기반 NAS 데이터 세트(NFS 또는 SMB), Amazon S3(Simple Storage Service) 오브젝트 형식, NetApp Cloud Sync ® 어플라이언스 또는 기타 클라우드 공급자 오브젝트 저장소 등 그 어떤 형태이든 변환 및 이동할 수 있습니다.

피처

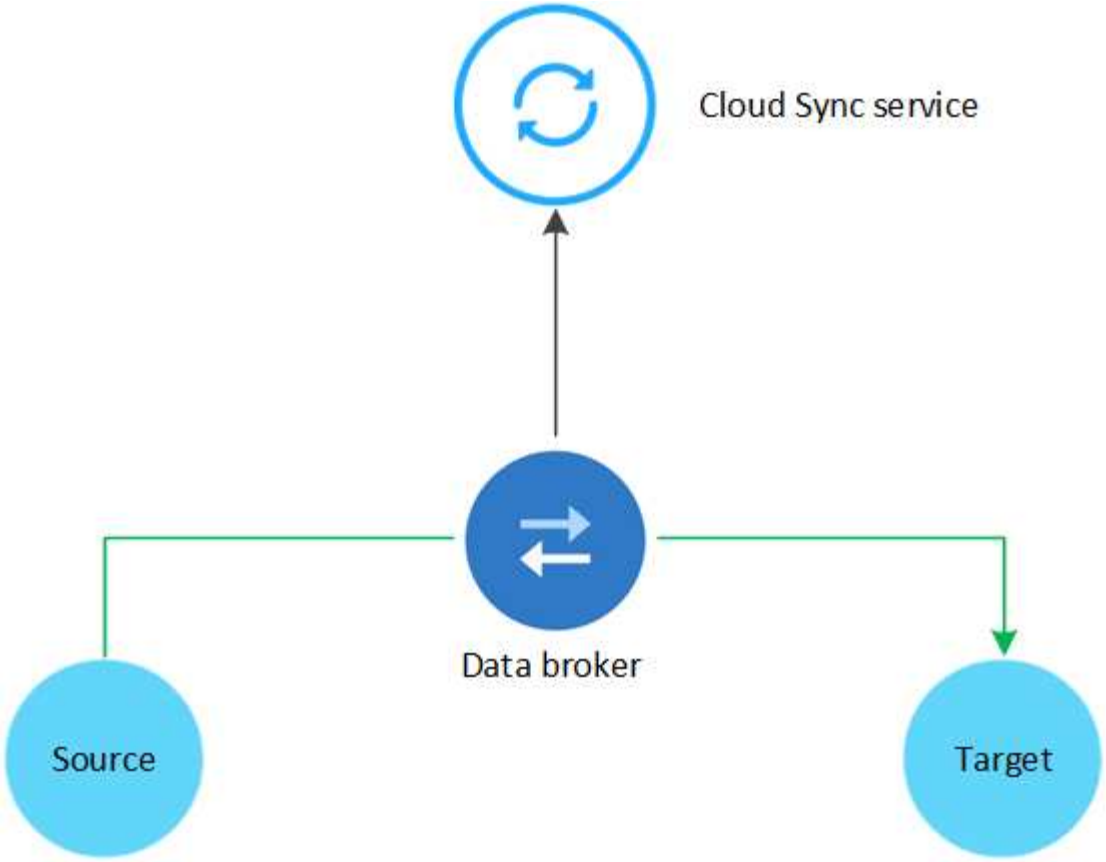
Cloud Sync에 대한 개요는 다음 비디오에서 확인할 수 있습니다.



Cloud Sync의 작동 방식

Cloud Sync는 데이터 브로커 그룹, Cloud Manager를 통해 사용 가능한 클라우드 기반 인터페이스, 소스 및 타겟으로 구성된 서비스형 소프트웨어(SaaS) 플랫폼입니다.

다음 이미지는 Cloud Sync 구성 요소 간의 관계를 보여줍니다.



NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(일명 A_SYNC Relationship _). AWS, Azure, Google Cloud Platform 또는 온프레미스에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 포트 443을 통한 아웃바운드 인터넷 연결이 있어야 Cloud Sync 서비스와 통신하고 몇 가지 다른 서비스 및 리포지토리에 연결할 수 있습니다. "끝점 목록을 봅니다".

초기 복사 후 서비스는 사용자가 설정한 일정에 따라 변경된 데이터를 동기화합니다.

지원되는 스토리지 유형입니다

Cloud Sync는 다음과 같은 스토리지 유형을 지원합니다.

- 모든 NFS 서버
- 모든 SMB 서버
- Amazon EFS
- ONTAP용 Amazon FSx
- Amazon S3
- Azure Blob
- Azure NetApp Files
- 상자(미리 보기로 사용 가능)
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google 클라우드 스토리지

- IBM 클라우드 오브젝트 스토리지
- 사내 ONTAP 클러스터
- ONTAP S3 스토리지
- SFTP(API만 사용)
- StorageGRID

"지원되는 동기화 관계를 봅니다".

비용

Cloud Sync 사용과 관련된 비용에는 리소스 비용 및 서비스 비용이라는 두 가지 유형이 있습니다.

리소스 비용

리소스 요금은 클라우드에서 하나 이상의 데이터 브로커를 실행하는 데 필요한 컴퓨팅 및 스토리지 비용과 관련이 있습니다.

서비스 요금

14일 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불할 수 있는 두 가지 방법이 있습니다. 첫 번째 옵션은 AWS 또는 Azure에서 가입하는 것입니다. 가입 서비스를 이용하면 시간 또는 연간 요금을 지불할 수 있습니다. 두 번째 옵션은 NetApp에서 직접 라이센스를 구매하는 것입니다.

"라이선스 작동 방식에 대해 알아보십시오".

Cloud Sync를 빠르게 시작합니다

Cloud Sync 서비스를 시작하는 데 몇 가지 단계가 포함되어 있습니다.

소스와 타겟이 지원되는지 확인하고 설정합니다. 가장 중요한 요구사항은 데이터 브로커 그룹과 소스 및 타겟 위치 간의 접속을 확인하는 것입니다.

- "지원되는 관계를 봅니다"
- "소스와 타겟을 준비합니다"

NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(일명 A_SYNC Relationship _). AWS, Azure, Google Cloud Platform 또는 온프레미스에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 포트 443을 통한 아웃바운드 인터넷 연결이 있어야 Cloud Sync 서비스와 통신하고 몇 가지 다른 서비스 및 리포지토리에 연결할 수 있습니다. "끝점 목록을 봅니다".

Cloud Sync는 동기화 관계를 생성할 때 설치 프로세스를 안내하며, 이 때 클라우드에 데이터 브로커를 구축하거나 자체 Linux 호스트에 대한 설치 스크립트를 다운로드할 수 있습니다.

- "AWS 설치를 검토합니다"
- "Azure 설치를 검토합니다"
- "Google Cloud 설치를 검토합니다"
- "Linux 호스트 설치를 검토합니다"

에 로그인합니다 "클라우드 관리자"를 클릭하고 * 동기화 * 를 클릭한 다음 선택한 소스 및 대상을 끌어서 놓습니다.

화면의 지시에 따라 설치를 완료합니다. "자세한 정보".

AWS 또는 Azure에서 가입하여 용량제 또는 연간 지불 가능합니다. 또는 NetApp에서 직접 라이센스를 구입합니다. Cloud Sync의 라이센스 설정 페이지로 이동하여 설정하기만 하면 됩니다. "자세한 정보".

지원되는 동기화 관계

Cloud Sync를 사용하면 소스에서 타겟으로 데이터를 동기화할 수 있습니다. 이를 동기화 관계라고 합니다. 시작하기 전에 지원되는 관계를 이해해야 합니다.

소스 위치	지원되는 타겟 위치
Amazon EFS	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID
ONTAP용 Amazon FSx	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID

소스 위치	지원되는 타겟 위치
Amazon S3	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID
Azure Blob	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID

소스 위치	지원되는 타겟 위치
Azure NetApp Files	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID
상자 [1]	• ONTAP용 Amazon FSx • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • SMB 서버 • StorageGRID

소스 위치	지원되는 타겟 위치
Cloud Volumes ONTAP	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID
Cloud Volumes Service	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID

소스 위치	지원되는 타겟 위치
Google 클라우드 스토리지	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • ONTAP S3 스토리지 • SMB 서버 • StorageGRID
IBM 클라우드 오브젝트 스토리지	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID

소스 위치	지원되는 타겟 위치
NFS 서버	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID
온프레미스 ONTAP 클러스터	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • SMB 서버 • StorageGRID
ONTAP S3 스토리지	• Google 클라우드 스토리지 • SMB 서버 • StorageGRID • ONTAP S3 스토리지
SFTP[2]	S3

소스 위치	지원되는 타겟 위치
SMB 서버	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • ONTAP S3 스토리지 • SMB 서버 • StorageGRID
StorageGRID	• Amazon EFS • ONTAP용 Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Google 클라우드 스토리지 • IBM 클라우드 오브젝트 스토리지 • NFS 서버 • 사내 ONTAP 클러스터 • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

참고:

1. Box 지원은 미리 보기로 제공됩니다.
2. 이 소스/타겟과의 관계 동기화는 Cloud Sync API만 사용하여 지원됩니다.

3. Blob 컨테이너가 타겟인 경우 특정 Azure Blob 저장소 계층을 선택할 수 있습니다.
    - 핫 스토리지
    - 멋진 보관
4. Amazon S3가 타겟일 때 특정 S3 스토리지 클래스를 선택할 수 있습니다.
    - 표준(기본 클래스)
    - 지능형 계층화
    - 표준 - 낮은 액세스 빈도
    - 단일 영역 - 낮은 액세스 빈도
    - 빙하
    - Glacier 딥 아카이브
5. Google Cloud Storage 버킷이 타겟인 경우 특정 스토리지 클래스를 선택할 수 있습니다.
    - 표준
    - 니어라인
    - 콜드라인
    - 아카이브

소스와 타겟을 준비합니다

소스와 타겟이 다음 요구 사항을 충족하는지 확인합니다.

네트워킹

- 소스와 타겟이 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

  예를 들어, NFS 서버가 데이터 센터에 있고 데이터 브로커가 AWS에 있는 경우 네트워크에서 VPC로 네트워크 연결(VPN 또는 Direct Connect)이 필요합니다.

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

대상 디렉토리

동기화 관계를 생성할 때 Cloud Sync를 사용하면 기존 타겟 디렉토리를 선택한 다음 필요에 따라 해당 디렉토리 내에 새 폴더를 생성할 수 있습니다. 따라서 선호하는 타겟 디렉토리가 이미 있는지 확인하십시오.

디렉토리를 읽을 수 있는 권한

소스 또는 타겟의 모든 디렉토리 또는 폴더를 표시하려면 Cloud Sync에서 디렉토리 또는 폴더에 대한 읽기 권한이 필요합니다.

NFS 를 참조하십시오

파일 및 디렉토리에 uid/gid가 있는 소스/대상에서 사용 권한을 정의해야 합니다.

오브젝트 스토리지

- AWS 및 Google Cloud의 경우 데이터 브로커에 목록 개체 권한이 있어야 합니다. 이러한 권한은 데이터 브로커 설치 단계를 수행하는 경우 기본적으로 제공됩니다.
- Azure, StorageGRID 및 IBM의 경우 동기화 관계를 설정할 때 입력하는 자격 증명에는 목록 개체 권한이 있어야 합니다.

중소기업

동기화 관계를 설정할 때 입력하는 SMB 자격 증명에는 목록 폴더 권한이 있어야 합니다.

데이터 브로커에서는 기본적으로 .snapshot,~snapshot,.copy-offload 디렉토리를 무시합니다

Amazon S3 버킷 요구 사항

Amazon S3 버킷이 다음 요구사항을 충족하는지 확인하십시오.

Amazon S3에 대해 지원되는 데이터 브로커 위치

S3 스토리지를 포함하는 동기화 관계는 AWS 또는 사내에 데이터 브로커가 배포되어야 합니다. 두 경우 모두 설치하는 동안 Cloud Sync에서 데이터 브로커를 AWS 계정에 연결하라는 메시지를 표시합니다.

- "AWS 데이터 브로커를 구축하는 방법을 알아보십시오"
- "Linux 호스트에 데이터 브로커를 설치하는 방법에 대해 알아보십시오"

지원되는 AWS 영역

중국 지역을 제외한 모든 지역이 지원됩니다.

다른 AWS 계정의 S3 버킷에 필요한 권한

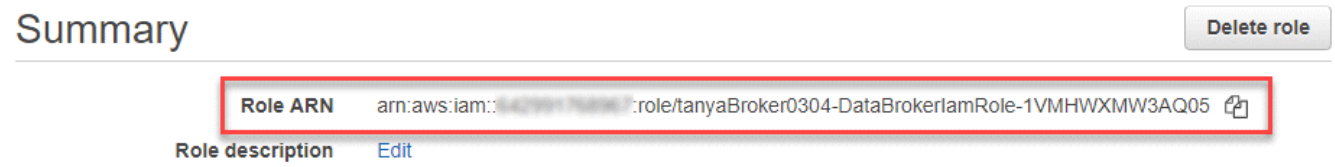
동기화 관계를 설정할 때 데이터 브로커와 연결되지 않은 AWS 계정에 상주하는 S3 버킷을 지정할 수 있습니다.

"이 JSON 파일에 포함된 권한" 데이터 브로커가 액세스할 수 있도록 이 S3 버킷에 적용해야 합니다. 이러한 사용 권한을 통해 데이터 브로커가 데이터를 버킷과 복사하거나 버킷의 오브젝트를 나열할 수 있습니다.

JSON 파일에 포함된 권한에 대해서는 다음을 참조하십시오.

1. _<BucketName>_은(는) 데이터 브로커와 연결되지 않은 AWS 계정에 상주하는 버킷의 이름입니다.
2. _<RoleARN>_은(는) 다음 중 하나로 교체해야 합니다.
   - 데이터 브로커가 Linux 호스트에 수동으로 설치된 경우, _RoleARN_은 데이터 브로커를 배포할 때 AWS 자격 증명을 제공한 AWS 사용자의 ARN 이어야 합니다.
   - CloudFormation 템플릿을 사용하여 AWS에 데이터 브로커가 배포된 경우, _RoleARN_은 템플릿에 의해 생성된 IAM 역할의 ARN 이어야 합니다.

     EC2 콘솔로 이동하여 데이터 브로커 인스턴스를 선택하고 설명 탭에서 IAM 역할을 클릭하여 역할 ARN을 찾을 수 있습니다. 그런 다음 IAM 콘솔에서 역할 ARN이 포함된 요약 페이지를 볼 수 있습니다.



Azure Blob 스토리지 요구 사항

Azure Blob 저장소가 다음 요구사항을 충족하는지 확인합니다.

Azure Blob에 지원되는 데이터 브로커 위치

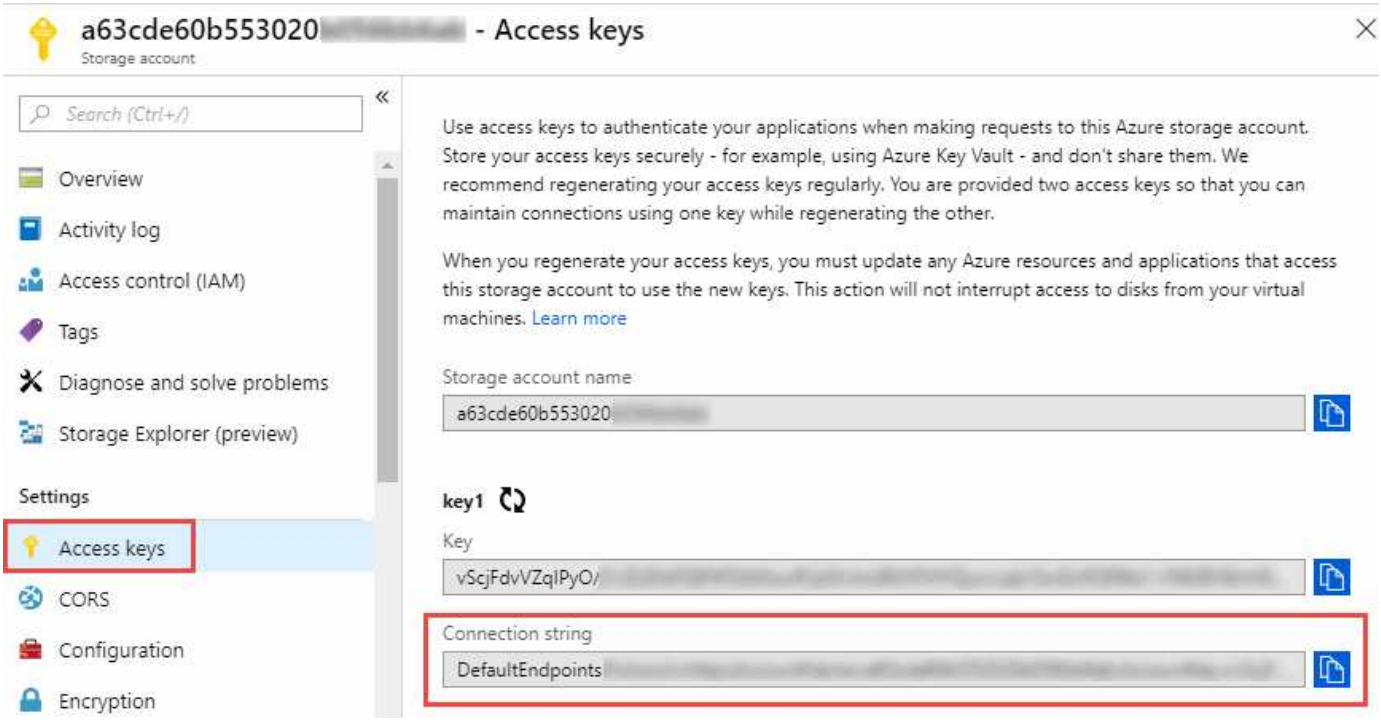
동기화 관계에 Azure Blob 스토리지가 포함된 경우 데이터 브로커가 모든 위치에 상주할 수 있습니다.

지원되는 Azure 지역

중국, 미국 정부 및 미국 국방부 지역을 제외한 모든 지역이 지원됩니다.

Azure Blob 및 NFS/SMB를 포함하는 관계의 연결 문자열

Azure Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화 관계를 생성할 때 Cloud Sync에 스토리지 계정 연결 문자열을 제공해야 합니다.

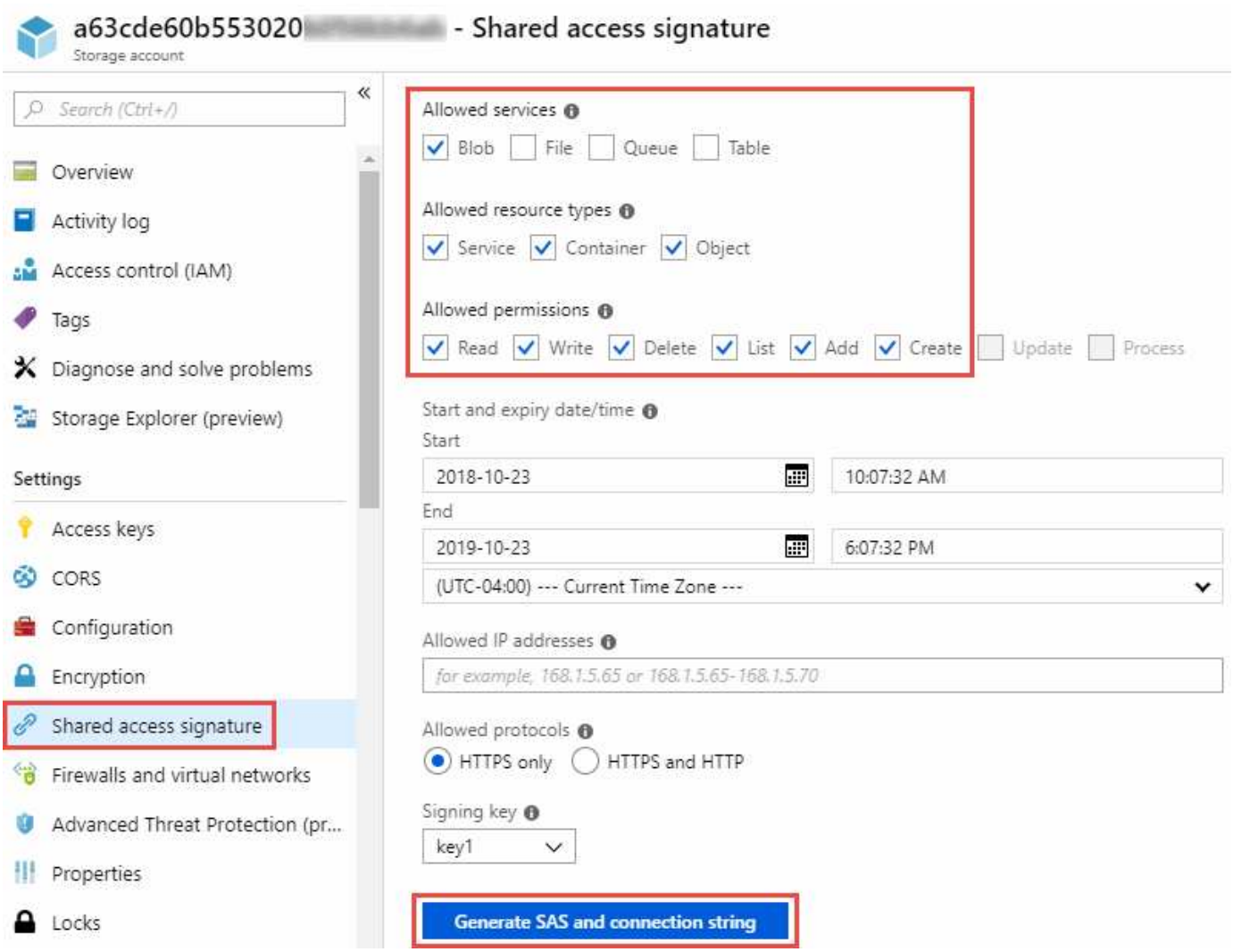


두 Azure Blob 컨테이너 간에 데이터를 동기화하려면 연결 문자열에 가 포함되어야 합니다 "공유 액세스 서명입니다" (SAS) Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화할 때 SAS를 사용할 수도 있습니다.

SAS는 Blob 서비스 및 모든 리소스 유형(서비스, 컨테이너 및 개체)에 대한 액세스를 허용해야 합니다. 또한 SAS에는 다음과 같은 사용 권한이 포함되어야 합니다.

- 소스 Blob 컨테이너의 경우 Read 및 List 입니다

- 대상 Blob 컨테이너의 경우 읽기, 쓰기, 목록, 추가 및 만들기 가 있습니다



Azure NetApp Files 요구 사항

Azure NetApp Files와 데이터를 동기화하거나에서 데이터를 동기화할 때 프리미엄 또는 울트라 서비스 수준을 사용합니다. 디스크 서비스 수준이 Standard인 경우 장애 및 성능 문제가 발생할 수 있습니다.

적합한 서비스 수준을 결정하는 데 도움이 필요한 경우 솔루션 설계자와 상의하십시오. 볼륨 크기와 볼륨 계층에 따라 처리량을 결정합니다.

"Azure NetApp Files 서비스 수준 및 처리량 에 대해 자세히 알아보십시오".

박스 요건

- Box를 포함하는 동기화 관계를 생성하려면 다음 자격 증명을 제공해야 합니다.
  - 클라이언트 ID입니다
  - 클라이언트 암호
  - 개인 키

- 공개 키 ID입니다
- 암호 구문
- 엔터프라이즈 ID입니다

- Amazon S3에서 Box로 동기화 관계를 생성하는 경우 다음 설정이 1로 설정된 통합 구성이 있는 데이터 브로커 그룹을 사용해야 합니다.
  - 스캐너 동시 사용
  - 스캐너 프로세스 제한
  - 운송 업체 위탁 통화
  - 수송 프로세스 제한

"데이터 브로커 그룹에 대한 통합 구성을 정의하는 방법에 대해 알아봅니다".

Google Cloud Storage 버킷 요구 사항

Google Cloud Storage 버킷이 다음 요구사항을 충족하는지 확인하십시오.

Google Cloud Storage에 대한 지원 데이터 브로커 위치

Google Cloud Storage를 포함한 동기화 관계에는 Google Cloud 또는 사내에 구축된 데이터 브로커가 필요합니다. Cloud Sync는 동기화 관계를 생성할 때 데이터 브로커 설치 프로세스를 안내합니다.

- "Google Cloud 데이터 브로커를 구축하는 방법을 알아보십시오"
- "Linux 호스트에 데이터 브로커를 설치하는 방법에 대해 알아보십시오"

지원되는 Google Cloud 지역

모든 지역이 지원됩니다.

다른 Google Cloud 프로젝트의 버킷에 대한 권한

동기화 관계를 설정할 때 데이터 브로커의 서비스 계정에 필요한 권한을 제공하는 경우 다양한 프로젝트의 Google Cloud 버킷 중에서 선택할 수 있습니다. "서비스 계정 설정 방법에 대해 알아보십시오".

SnapMirror 대상에 대한 권한입니다

동기화 관계의 소스가 SnapMirror 대상(읽기 전용)인 경우 "읽기/목록" 사용 권한으로 소스의 데이터를 타겟으로 동기화할 수 있습니다.

NFS 서버 요구 사항

- NFS 서버는 NetApp 시스템이거나 NetApp이 아닌 시스템이 될 수 있습니다.
- 파일 서버는 데이터 브로커 호스트가 필요한 포트를 통해 내보내기에 액세스할 수 있도록 허용해야 합니다.
  - 111 TCP/UDP
  - 2049 TCP/UDP
  - 5555 TCP/UDP

- NFS 버전 3, 4.0, 4.1 및 4.2가 지원됩니다.

  서버에서 원하는 버전을 활성화해야 합니다.

- ONTAP 시스템에서 NFS 데이터를 동기화하려면 SVM을 위한 NFS 내보내기 목록에 대한 액세스가 활성화되어 있는지 확인하십시오(vserver NFS modify -vserver_svm_name_-showmount 설정).

  showmount의 기본 설정은 ONTAP 9.2부터 _enabled_입니다.

ONTAP 요구 사항

동기화 관계에 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터가 포함되어 있고 NFSv4 이상을 선택한 경우 ONTAP 시스템에서 NFSv4 ACL을 설정해야 합니다. ACL을 복제하려면 이 작업이 필요합니다.

ONTAP S3 스토리지 요구 사항

을 포함하는 동기화 관계를 설정할 때 "ONTAP S3 스토리지"다음을 제공해야 합니다.

- ONTAP S3에 연결된 LIF의 IP 주소입니다
- ONTAP에서 사용하도록 구성된 액세스 키 및 암호 키입니다

SMB 서버 요구 사항

- SMB 서버는 NetApp 시스템 또는 NetApp이 아닌 시스템일 수 있습니다.
- SMB 서버에 대한 권한이 있는 자격 증명을 Cloud Sync에 제공해야 합니다.
  - 소스 SMB 서버의 경우 목록 및 읽기 권한이 필요합니다.

    Backup Operators 그룹의 구성원은 소스 SMB 서버에서 지원됩니다.

  - 대상 SMB 서버의 경우 목록, 읽기 및 쓰기의 권한이 필요합니다.
- 파일 서버는 데이터 브로커 호스트가 필요한 포트를 통해 내보내기에 액세스할 수 있도록 허용해야 합니다.
  - 139 TCP 를 참조하십시오
  - 445 TCP
  - 137-138 UDP
- SMB 버전 1.0, 2.0, 2.1, 3.0 및 3.11이 지원됩니다.
- "Administrators" 그룹에 소스 및 대상 폴더에 "모든 권한" 권한을 부여합니다.

  이 권한을 부여하지 않으면 데이터 브로커에 파일 또는 디렉터리에 대한 ACL을 가져올 수 있는 권한이 충분하지 않을 수 있습니다. 이 경우 "getxattr error 95" 오류가 발생합니다.

숨겨진 디렉토리 및 파일에 대한 **SMB** 제한

SMB 제한은 SMB 서버 간에 데이터를 동기화할 때 숨겨진 디렉터리 및 파일에 영향을 줍니다. 소스 SMB 서버의 디렉토리 또는 파일이 Windows를 통해 숨겨진 경우 숨겨진 속성은 타겟 SMB 서버로 복제되지 않습니다.

대소문자 구분 제한 때문에 **SMB** 동기화 동작이 발생합니다

SMB 프로토콜은 대/소문자를 구분하지 않으므로 대문자와 소문자가 동일하게 처리됩니다. 이 동작은 동기화 관계에 SMB 서버가 포함되어 있고 데이터가 이미 타겟에 존재하는 경우 덮어쓴 파일 및 디렉토리 복사 오류를 발생시킬 수 있습니다.

예를 들어, 소스에 "A"라는 파일이 있고 대상에 "A"라는 이름의 파일이 있다고 가정해 보겠습니다. Cloud Sync가 "A"라는 파일을 대상에 복사하면 파일 "A"가 소스의 파일 "A"에 의해 덮어쓰여집니다.

디렉토리의 경우 소스에 "b"라는 디렉토리가 있고 타겟에 "B"라는 디렉토리가 있다고 가정해 보겠습니다. Cloud Sync가 "b"라는 디렉토리를 타겟으로 복제하려고 하면 Cloud Sync에서 디렉토리가 이미 존재함을 나타냅니다. 따라서 Cloud Sync는 항상 "b"라는 이름의 디렉토리를 복사하지 못합니다.

이 제한을 피하는 가장 좋은 방법은 데이터를 빈 디렉토리에 동기화하는 것입니다.

Cloud Sync의 네트워킹 개요

Cloud Sync용 네트워킹에는 데이터 브로커 그룹과 소스 및 대상 위치 간의 연결과 포트 443을 통한 데이터 브로커로부터의 아웃바운드 인터넷 연결이 포함됩니다.

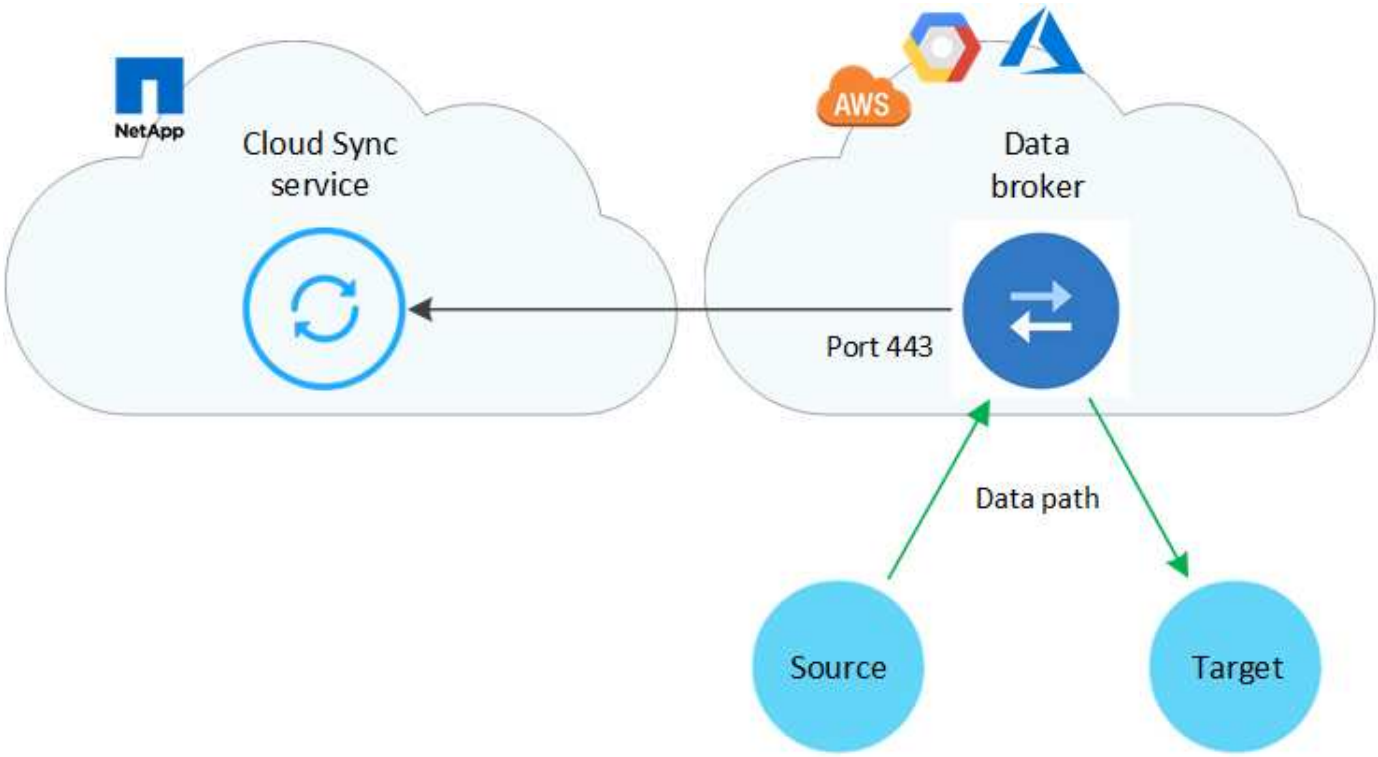
데이터 브로커 위치

데이터 브로커 그룹은 클라우드 또는 사내에 설치되는 하나 이상의 데이터 브로커로 구성됩니다.

클라우드 내 데이터 브로커

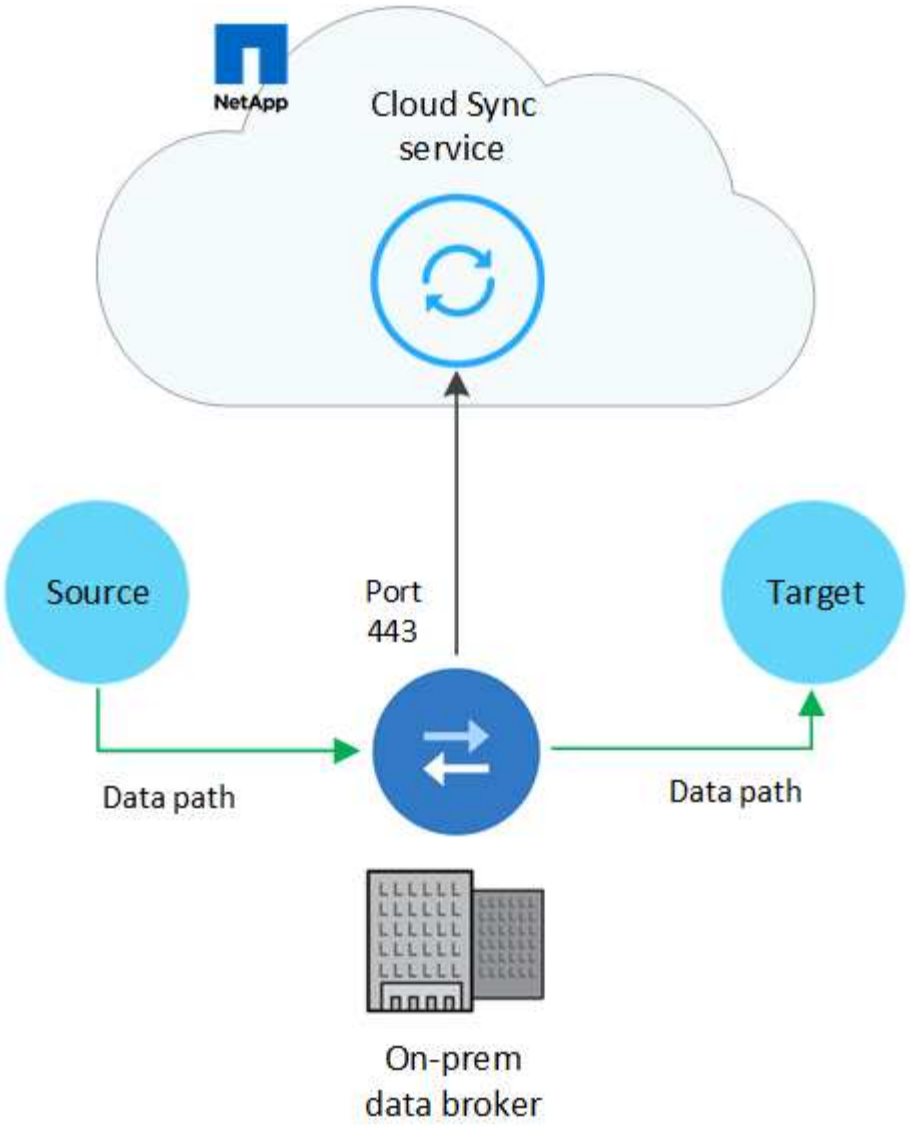
다음 이미지는 AWS, Google Cloud 또는 Azure에서 클라우드에서 실행 중인 데이터 브로커를 보여줍니다. 데이터 브로커에 대한 연결이 있는 한 소스와 타겟이 모든 위치에 있을 수 있습니다. 예를 들어, 데이터 센터와 클라우드 공급자에 VPN 연결을 설정할 수 있습니다.

Cloud Sync은 AWS, Azure 또는 Google Cloud에 데이터 브로커를 구축할 경우 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.



사내 데이터 브로커

다음 이미지는 사내 데이터 센터에서 실행되는 데이터 브로커를 보여줍니다. 다시 한 번 말씀드리지만, 데이터 브로커에 대한 연결이 있는 한 소스 및 타겟이 모든 위치에 있을 수 있습니다.



네트워킹 요구 사항

- 소스와 타겟이 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

  예를 들어, NFS 서버가 데이터 센터에 있고 데이터 브로커가 AWS에 있는 경우 네트워크에서 VPC로 네트워크 연결(VPN 또는 Direct Connect)이 필요합니다.

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.
- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

네트워킹 엔드포인트

NetApp 데이터 브로커는 포트 443을 통한 아웃바운드 인터넷 액세스를 통해 Cloud Sync 서비스와 통신하고 몇 가지 다른 서비스 및 리포지토리에 연락해야 합니다. 로컬 웹 브라우저에서도 특정 작업을 수행하려면 끝점에 액세스해야 합니다. 아웃바운드 연결을 제한해야 하는 경우 아웃바운드 트래픽에 대해 방화벽을 구성할 때 다음 엔드포인트 목록을 참조하십시오.

데이터 브로커 엔드포인트

데이터 브로커가 다음 엔드포인트에 연결합니다.

엔드포인트	목적
https://olcentgbl.trafficmanager.net 으로 문의하십시오	데이터 브로커 호스트의 CentOS 패키지를 업데이트하기 위해 리포지토리에 접속하려면 이 엔드포인트는 CentOS 호스트에 데이터 브로커를 수동으로 설치하는 경우에만 연결됩니다.
https://rpm.nodesource.com https://registry.npmjs.org https://nodejs.org: 를 참조하십시오	개발에 사용되는 Node.js, NPM 및 기타 타사 패키지를 업데이트하기 위한 리포지토리에 접속합니다.
https://tgz.pm2.io 으로 문의하십시오	Cloud Sync를 모니터링하는 데 사용되는 타사 패키지인 PM2를 업데이트하기 위한 리포지토리에 액세스합니다.
https://sqs.us-east-1.amazonaws.com https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	Cloud Sync에서 운영에 사용하는 AWS 서비스(파일 대기열 처리, 작업 등록, 데이터 브로커에 업데이트 제공)에 연락하려면
https://s3.*region*.amazonaws.com 예: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["S3 엔드포인트 목록은 AWS 설명서를 참조하십시오"^]	동기화 관계에 S3 버킷이 포함된 경우 Amazon S3에 연락하려면
https://s3.us-east-1.amazonaws.com 으로 문의하십시오	Cloud Sync에서 데이터 브로커 로그를 다운로드하면 데이터 브로커가 로그 디렉토리를 지퍼하고 로그를 us-east-1 지역의 미리 정의된 S3 버킷으로 업로드합니다.
https://cf.cloudsync.netapp.com https://repo.cloudsync.netapp.com 으로 문의하십시오	Cloud Sync 서비스에 문의하십시오.
https://support.netapp.com 으로 문의하십시오	BYOL 라이센스를 사용하여 동기화 관계에 대한 NetApp 지원 팀에 문의
https://fedoraproject.org 으로 문의하십시오	설치 및 업데이트 중에 데이터 브로커 가상 머신에 7z를 설치하려면 다음을 수행합니다. 7z는 NetApp 기술 지원 팀에 AutoSupport 메시지 전송 기능이 필요합니다.
https://sts.amazonaws.com 으로 문의하십시오	데이터 브로커가 AWS에 구축되거나 사내 구축 시에 AWS 자격 증명이 제공되고 AWS 자격 증명이 제공됩니다. 데이터 브로커가 배포, 업데이트 및 재시작 중에 이 엔드포인트에 연결합니다.
https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com 으로 문의하십시오	데이터 센스를 사용하여 새 동기화 관계를 위한 소스 파일을 선택할 때 클라우드 데이터 센스에 문의하려면

웹 브라우저 끝점

문제 해결을 위해 로그를 다운로드하려면 웹 브라우저에서 다음 끝점에 액세스해야 합니다.

logs.cloudsync.netapp.com:443

데이터 브로커를 설치합니다

AWS에서 새 데이터 브로커 생성

새 데이터 브로커 그룹을 생성하는 경우 Amazon Web Services 를 선택하여 VPC의 새 EC2 인스턴스에 데이터 브로커 소프트웨어를 배포합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

클라우드 또는 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치할 수도 있습니다. "자세한 정보".

지원되는 AWS 영역

중국 지역을 제외한 모든 지역이 지원됩니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Cloud Sync는 AWS에 데이터 브로커를 구축할 때 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다. 설치 프로세스 중에 프록시 서버를 사용하도록 데이터 브로커를 구성할 수 있습니다.

  아웃바운드 연결을 제한해야 하는 경우 를 참조하십시오 "데이터 브로커가 연락하는 끝점 목록입니다".

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

AWS에서 데이터 브로커를 구축하는 데 필요한 권한입니다

데이터 브로커를 구축하는 데 사용하는 AWS 사용자 계정에 에 포함된 권한이 있어야 합니다 "NetApp에서 제공하는 정책입니다".

AWS 데이터 브로커와 함께 IAM 역할을 사용해야 합니다

Cloud Sync는 데이터 브로커를 배포할 때 데이터 브로커 인스턴스에 대해 IAM 역할을 생성합니다. 원할 경우 자체 IAM 역할을 사용하여 데이터 브로커를 배포할 수 있습니다. 조직에 엄격한 보안 정책이 있는 경우 이 옵션을 사용할 수 있습니다.

IAM 역할은 다음 요구 사항을 충족해야 합니다.

- IAM 역할을 신뢰할 수 있는 엔터티로 사용하려면 EC2 서비스가 허용되어야 합니다.
- "이 JSON 파일에 정의된 권한" 데이터 브로커가 올바르게 작동할 수 있도록 IAM 역할에 연결해야 합니다.

데이터 브로커를 배포할 때 IAM 역할을 지정하려면 아래 단계를 따르십시오.

데이터 브로커 생성

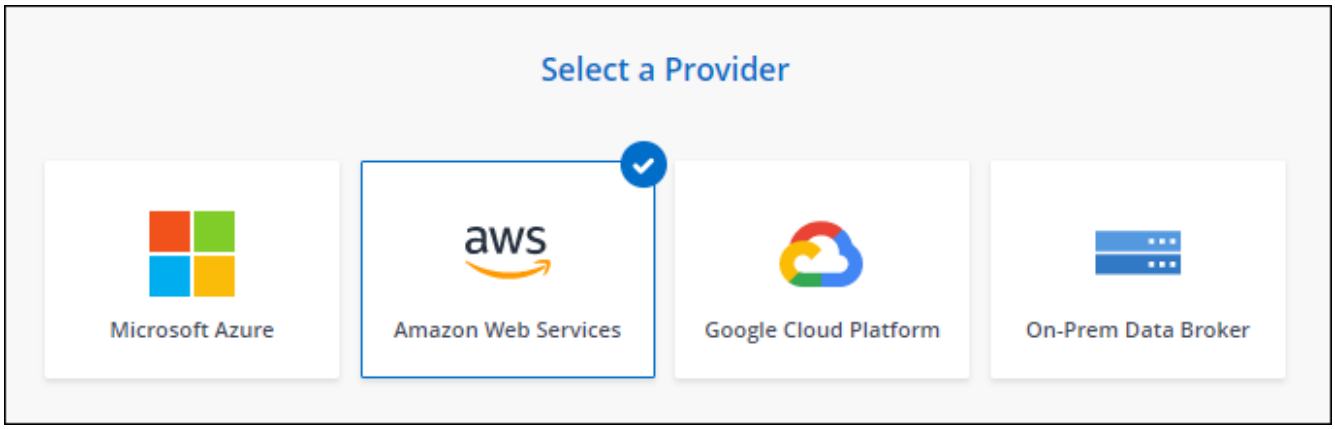
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 생성할 때 AWS에서 데이터 브로커를 설치하는 방법을 설명합니다.

단계

1. 새 동기화 만들기 * 를 클릭합니다.
2. 동기화 관계 정의 * 페이지에서 소스 및 대상을 선택하고 * 계속 * 을 클릭합니다.

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 * 페이지에서 * 데이터 브로커 * 생성 을 클릭한 다음 * Amazon Web Services * 를 선택합니다.



4. 데이터 브로커의 이름을 입력하고 * 계속 * 을 클릭합니다.
5. AWS 액세스 키를 입력하여 Cloud Sync에서 대신 AWS에서 데이터 브로커를 생성할 수 있습니다.

   키는 다른 용도로 저장되거나 사용되지 않습니다.

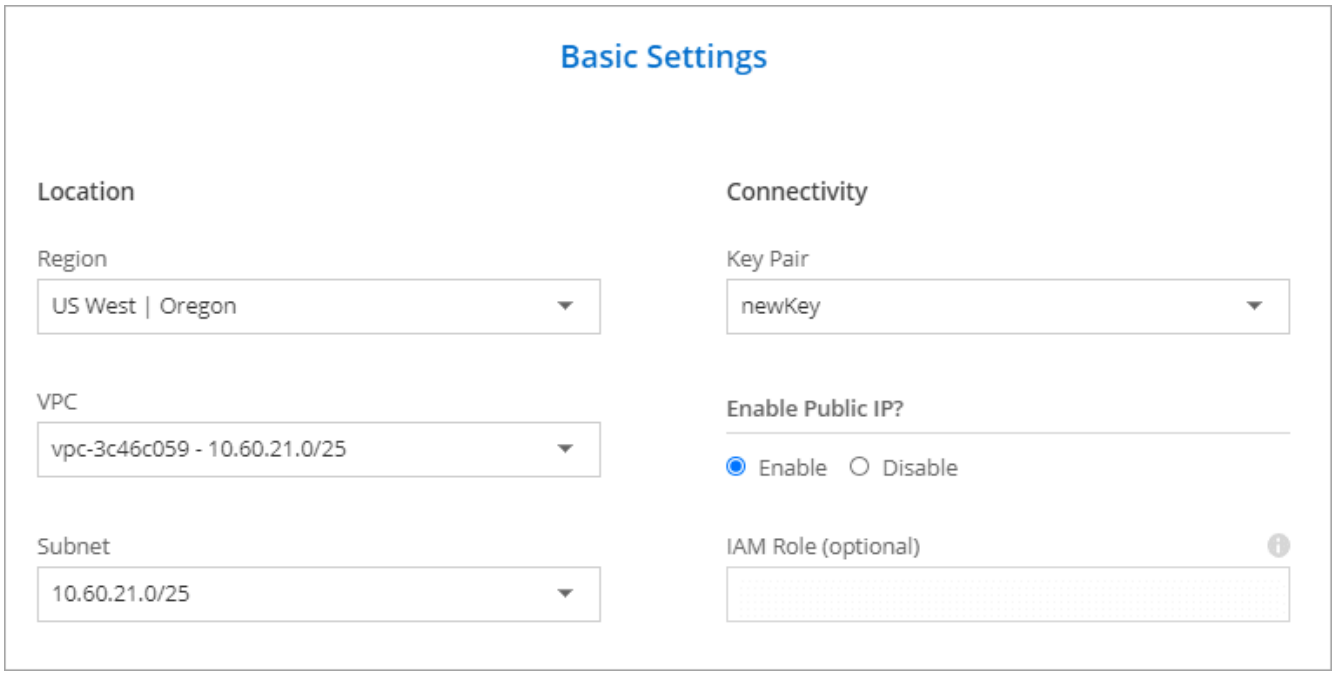
   액세스 키를 제공하지 않고 싶은 경우 페이지 하단에 있는 링크를 클릭하여 CloudFormation 템플릿을 대신 사용하십시오. 이 옵션을 사용할 경우 AWS에 직접 로그인하므로 자격 증명을 제공할 필요가 없습니다.

   다음 비디오에서는 CloudFormation 템플릿을 사용하여 데이터 브로커 인스턴스를 시작하는 방법을 설명합니다.

   ► https://docs.netapp.com/ko-kr/cloud-manager-sync//media/video_cloud_sync.mp4 *(video)*

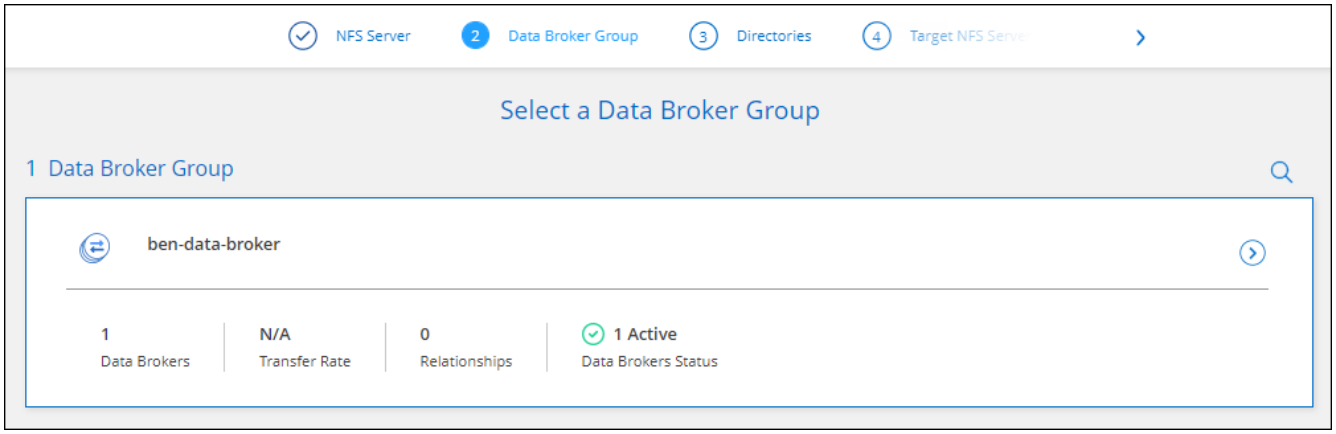
6. AWS 액세스 키를 입력한 경우, 인스턴스에 대한 위치를 선택하고 키 쌍을 선택한 다음 공용 IP 주소 활성화 여부를 선택한 다음 기존 IAM 역할을 선택하거나 필드를 비워 Cloud Sync에서 역할을 생성합니다.

   IAM 역할을 직접 선택할 경우 필요한 권한을 제공해야 합니다.



7. VPC의 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.
8. 데이터 브로커를 사용할 수 있게 되면 Cloud Sync에서 * 계속 * 을 클릭합니다.

   다음 이미지는 AWS에 성공적으로 구축된 인스턴스를 보여줍니다.



9. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

AWS에 데이터 브로커를 구축하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브로커 그룹을 추가 동기화 관계에 사용할 수 있습니다.

데이터 브로커 인스턴스에 대한 세부 정보

Cloud Sync은 다음 구성을 사용하여 AWS에서 데이터 브로커를 생성합니다.

인스턴스 유형

m5n.xlarge(m5n.xlarge)(해당 지역에서 사용할 수 있는 경우), 그렇지 않은 경우 m5.xlarge

vCPU
4

RAM
16GB

운영 체제
Amazon Linux 2

디스크 크기 및 유형입니다
10GB GP2 SSD

Azure에서 새 데이터 브로커 생성

새 데이터 브로커 그룹을 생성할 때 Microsoft Azure를 선택하여 VNET의 새 가상 머신에 데이터 브로커 소프트웨어를 배포합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

클라우드 또는 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치할 수도 있습니다. "자세한 정보".

지원되는 **Azure** 지역

중국, 미국 정부 및 미국 국방부 지역을 제외한 모든 지역이 지원됩니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Cloud Sync는 Azure에 데이터 브로커를 배포할 때 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.

  아웃바운드 연결을 제한해야 하는 경우 를 참조하십시오 "데이터 브로커가 연락하는 끝점 목록입니다".

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

Azure에서 데이터 브로커를 배포하는 데 필요한 권한입니다

데이터 브로커를 배포하는 데 사용하는 Azure 사용자 계정에 다음과 같은 권한이 있는지 확인합니다.

```
{
    "Name": "Azure Data Broker",
    "Actions": [
                    "Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/deployments/operationstatuses/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
```

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Resources/deployments/cancel/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/publicIPAddresses/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",

"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/virtualNetworks/read",
                    "Microsoft.Network/publicIPAddresses/write",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/publicIPAddresses/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Network/publicIPAddresses/join/action",
                    "Microsoft.Network/networkInterfaces/join/action"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}
```

인증 방법

데이터 브로커를 구축할 때는 가상 머신의 인증 방법, 즉 암호 또는 SSH 공개-개인 키 쌍을 선택해야 합니다.

키 쌍 생성에 대한 도움말은 을 참조하십시오 "Azure 설명서: Azure에서 Linux VM용 SSH 공개-개인 키 쌍을 생성하고 사용합니다".

데이터 브로커 생성

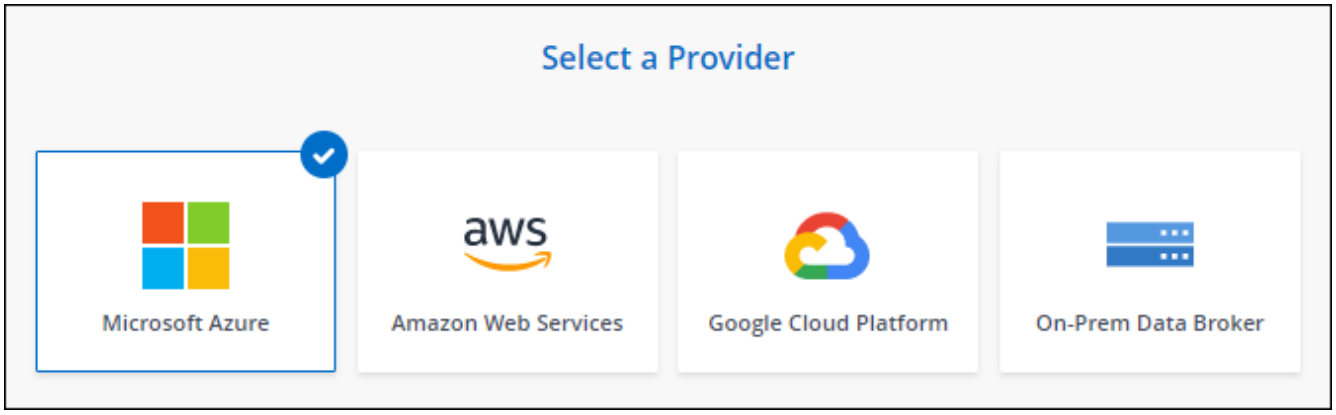
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 만들 때 Azure에서 데이터 브로커를 설치하는 방법을 설명합니다.

단계

1. 새 동기화 만들기 * 를 클릭합니다.
2. 동기화 관계 정의 * 페이지에서 소스 및 대상을 선택하고 * 계속 * 을 클릭합니다.

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

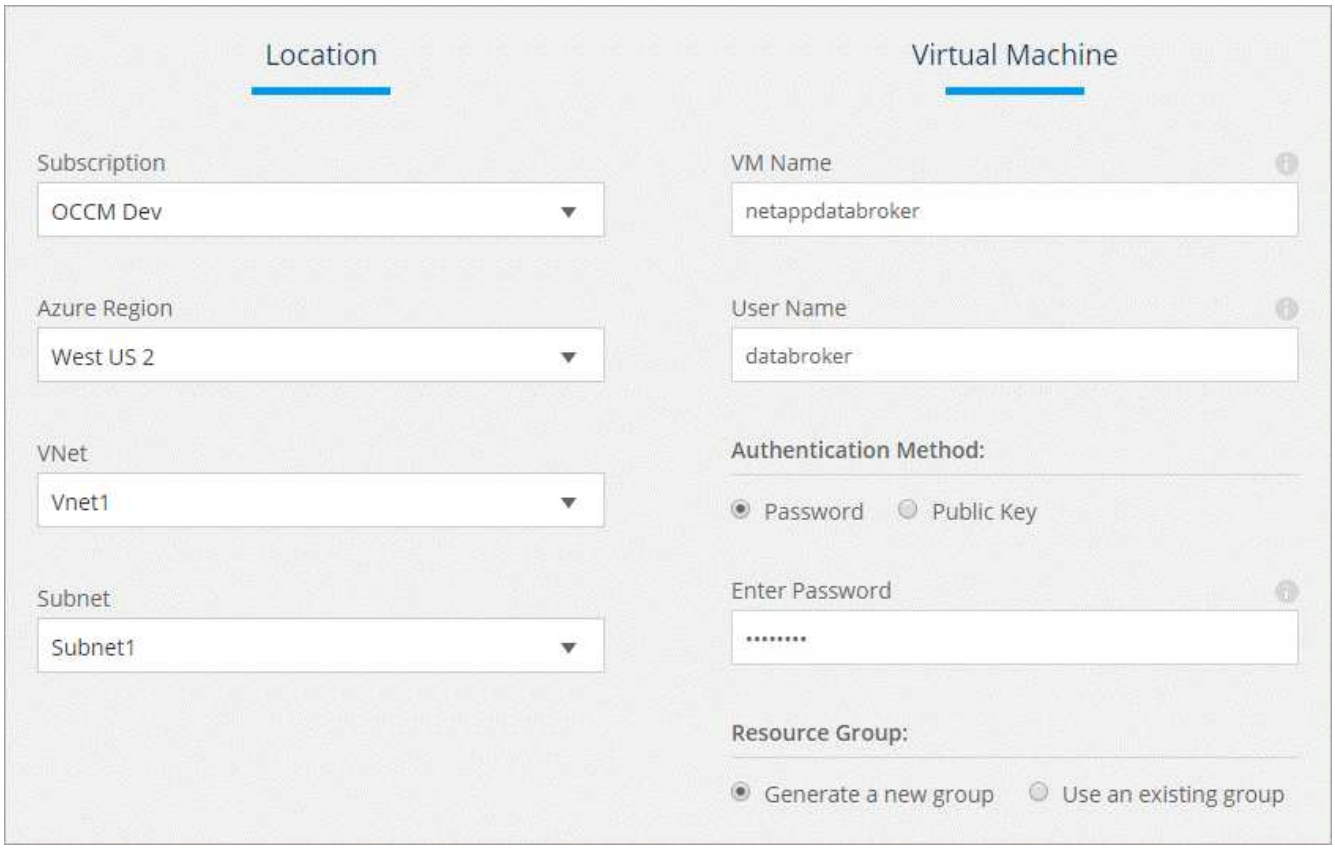
3. 데이터 브로커 그룹 * 페이지에서 * 데이터 브로커 * 만들기 를 클릭한 다음 * Microsoft Azure * 를 선택합니다.



4. 데이터 브로커의 이름을 입력하고 * 계속 * 을 클릭합니다.
5. 메시지가 표시되면 Microsoft 계정에 로그인합니다. 메시지가 표시되지 않으면 * Azure에 로그인 * 을 클릭합니다.

   이 양식은 Microsoft에서 소유하고 호스팅됩니다. 자격 증명이 NetApp에 제공되지 않습니다.

6. 데이터 브로커의 위치를 선택하고 가상 시스템에 대한 기본 세부 정보를 입력합니다.



7. VNET에서 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.
8. 계속 * 을 클릭하고 배포가 완료될 때까지 페이지를 열어 둡니다.

   이 프로세스는 최대 7분 정도 소요될 수 있습니다.

9. Cloud Sync에서 데이터 브로커를 사용할 수 있게 되면 * 계속 * 을 클릭합니다.
10. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

Azure에서 데이터 브로커를 구축하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브로커를 추가 동기화 관계에 사용할 수 있습니다.

관리자 동의가 필요하다는 메시지를 받았습니까?

Cloud Sync에서 사용자 대신 조직의 리소스에 액세스할 수 있는 권한이 필요하므로 관리자 승인이 필요하다는 메시지가 나타나면 다음 두 가지 옵션을 사용할 수 있습니다.

1. AD 관리자에게 다음 권한을 제공하도록 요청하십시오.

   Azure에서 * 관리 센터 > Azure AD > 사용자 및 그룹 > 사용자 설정 * 으로 이동하여 * 사용자가 회사 데이터에 액세스하는 앱에 대신 * 사용자 동의를 할 수 있습니다 *.

2. AD 관리자에게 다음 URL(관리자 동의 엔드포인트)을 사용하여 * CloudSync-AzureDataBrokerCreator * 에 대해 사용자 대신 동의하도록 요청하십시오.

   https://login.microsoftonline.com/{FILL 여기서 귀하의 테넌트 ID}
   /v2.0/adminConsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85 &
   redirect_Uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   URL에 표시된 것처럼 앱 URL은 https://cloudsync.netapp.com 이고 응용 프로그램 클라이언트 ID는 8ee4ca3a-bafa-4831-97cc-5a38923cab85입니다.

데이터 브로커 **VM**에 대한 세부 정보

Cloud Sync는 다음 구성을 사용하여 Azure에서 데이터 브로커를 생성합니다.

VM 유형입니다
: 표준 DS4 v2

vCPU
: 8

RAM
: 28GB

운영 체제
: CentOS 7.7

디스크 크기 및 유형입니다
: 64GB 프리미엄 SSD

Google Cloud에서 새로운 데이터 브로커 생성

새 데이터 브로커 그룹을 생성하는 경우 Google Cloud Platform 을 선택하여 Google Cloud VPC의 새 가상 머신 인스턴스에 데이터 브로커 소프트웨어를 배포합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

클라우드 또는 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치할 수도 있습니다. "자세한 정보".

지원되는 **Google Cloud** 지역

모든 지역이 지원됩니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Cloud Sync가 Google Cloud에 데이터 브로커를 배포할 때 필요한 아웃바운드 통신을 지원하는 보안 그룹을 만듭니다.

  아웃바운드 연결을 제한해야 하는 경우 를 참조하십시오 "데이터 브로커가 연락하는 끝점 목록입니다".

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

Google Cloud에서 데이터 브로커를 배포하는 데 필요한 권한입니다

데이터 브로커를 배포하는 Google Cloud 사용자에게 다음과 같은 권한이 있는지 확인합니다.

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

서비스 계정에 필요한 권한입니다

데이터 브로커를 배포할 때 다음과 같은 권한이 있는 서비스 계정을 선택해야 합니다.

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
- iam.serviceAccounts.signJwt
```

"iam.serviceAccounts.signJwt" 권한은 외부 HashashCorp 볼트를 사용하도록 데이터 브로커를 설정할 계획에만 필요합니다.

데이터 브로커 생성

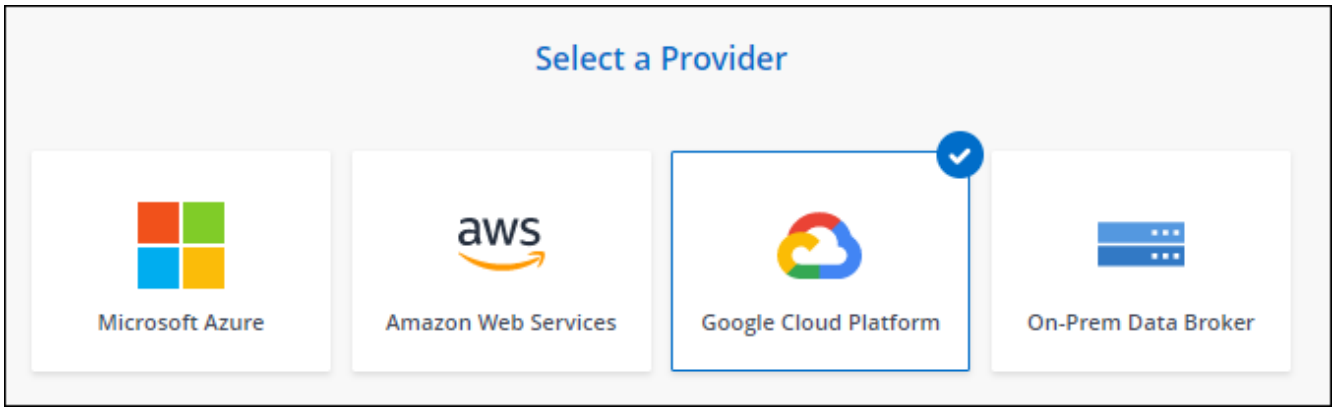
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 생성할 때 Google Cloud에 데이터 브로커를 설치하는 방법을 설명합니다.

단계

1. 새 동기화 만들기 * 를 클릭합니다.
2. 동기화 관계 정의 * 페이지에서 소스 및 대상을 선택하고 * 계속 * 을 클릭합니다.

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 * 페이지에서 * 데이터 브로커 * 만들기 를 클릭한 다음 * Microsoft Azure * 를 선택합니다.

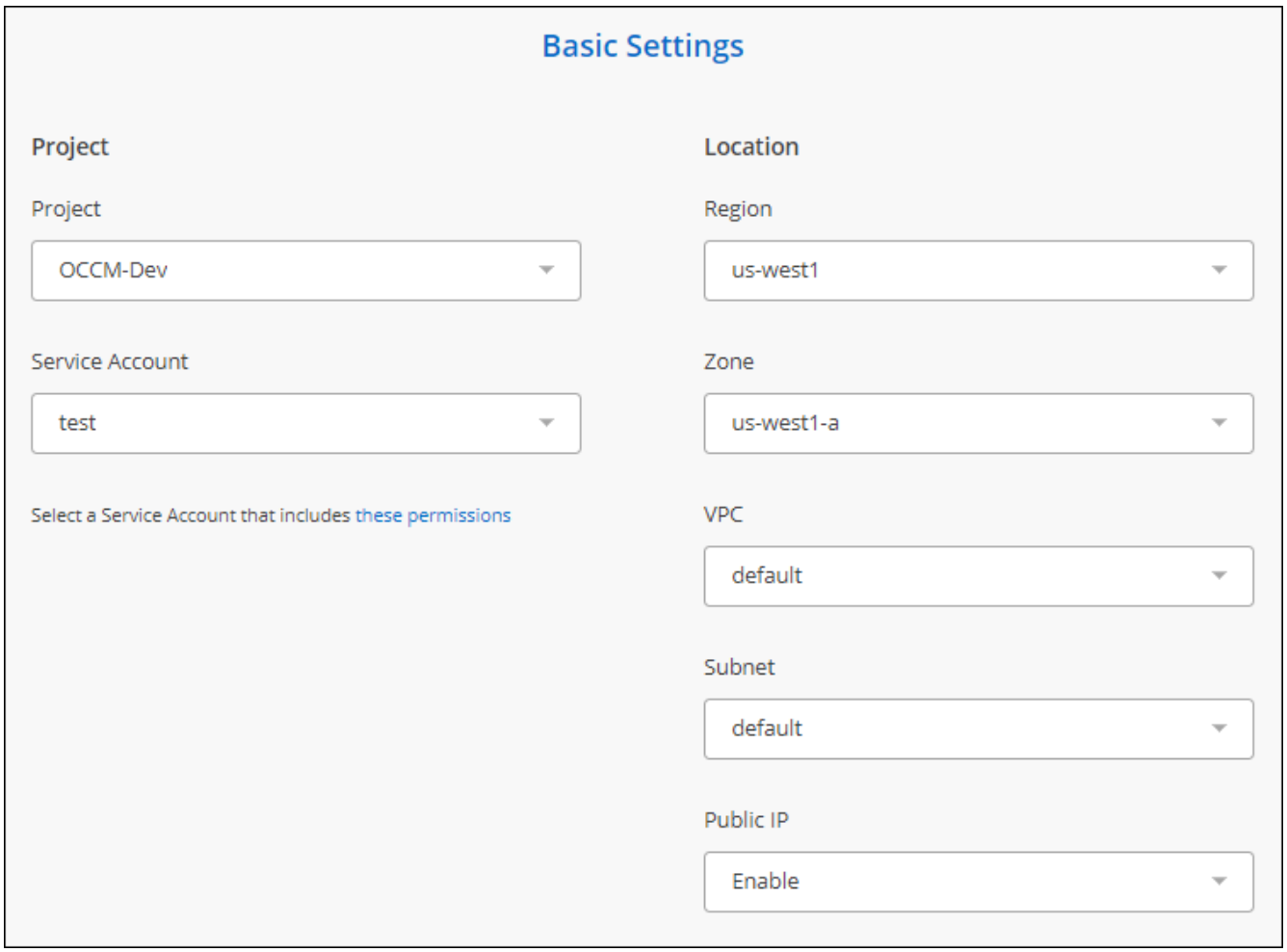


4. 데이터 브로커의 이름을 입력하고 * 계속 * 을 클릭합니다.
5. 메시지가 표시되면 Google 계정으로 로그인합니다.

   이 양식은 Google에서 소유하고 호스팅됩니다. 자격 증명이 NetApp에 제공되지 않습니다.

6. 프로젝트 및 서비스 계정을 선택한 다음 공용 IP 주소 활성화 또는 비활성화 여부를 포함하여 데이터 브로커의 위치를 선택합니다.

   공용 IP 주소를 사용하지 않는 경우 다음 단계에서 프록시 서버를 정의해야 합니다.



7. VPC의 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.

   인터넷 액세스에 프록시가 필요한 경우 프록시는 Google Cloud에 있어야 하며 데이터 브로커와 동일한 서비스 계정을 사용해야 합니다.

8. 데이터 브로커를 사용할 수 있게 되면 Cloud Sync에서 * 계속 * 을 클릭합니다.

   인스턴스를 구축하는 데 약 5~10분이 소요됩니다. Cloud Sync 서비스에서 진행 상황을 모니터링할 수 있으며, 이 경우 인스턴스를 사용할 수 있을 때 자동으로 새로 고쳐집니다.

9. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

Google Cloud에 데이터 브로커를 구축하고 새로운 동기화 관계를 구축했습니다. 이 데이터 브로커를 추가 동기화 관계에 사용할 수 있습니다.

다른 **Google Cloud** 프로젝트에 버킷을 사용할 수 있는 권한 제공

동기화 관계를 생성하고 Google 클라우드 스토리지를 소스 또는 타겟으로 선택할 때, Cloud Sync을 사용하면 데이터 브로커의 서비스 계정에 사용할 수 있는 버킷 중에서 선택할 수 있습니다. 기본적으로 여기에는 데이터 브로커 서비스 계정과 _Same_PROJECT 에 있는 버킷이 포함됩니다. 그러나 필요한 권한을 제공하는 경우 _other_projects 에서 버킷을 선택할 수 있습니다.

단계

1. Google Cloud Platform 콘솔을 열고 클라우드 스토리지 서비스를 로드합니다.

2. 동기화 관계에서 소스 또는 타겟으로 사용할 버킷의 이름을 클릭합니다.
3. 사용 권한 * 을 클릭합니다.
4. 추가 * 를 클릭합니다.
5. 데이터 브로커의 서비스 계정 이름을 입력합니다.
6. 에서 제공하는 역할을 선택합니다 위와 동일한 권한.
7. 저장 * 을 클릭합니다.

동기화 관계를 설정하면 이제 해당 버킷을 동기화 관계의 소스 또는 타겟으로 선택할 수 있습니다.

데이터 브로커 **VM** 인스턴스에 대한 세부 정보

Cloud Sync은 다음 구성을 사용하여 Google Cloud에서 데이터 브로커를 생성합니다.

기계 유형
: N1-표준-4

vCPU
: 4

RAM
: 15GB

운영 체제
: Red Hat Enterprise Linux 7.7

디스크 크기 및 유형입니다
: 20GB HDD PD 표준

Linux 호스트에 데이터 브로커 설치

새 데이터 브로커 그룹을 생성할 때 사내 Linux 호스트 또는 클라우드의 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치하려면 온프레미스 데이터 브로커 옵션을 선택합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

Linux 호스트 요구 사항

- * 운영 체제 *:
  - CentOS 7.0, 7.7 및 8.0

    CentOS 스트림은 지원되지 않습니다.
  - Red Hat Enterprise Linux 7.7 및 8.0
  - Ubuntu 서버 20.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

데이터 브로커를 설치하기 전에 호스트에서 'yum update all' 명령을 실행해야 합니다.

Red Hat Enterprise Linux 시스템은 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우, 시스템은 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

- RAM *: 16GB
- * CPU *: 4코어
- * 여유 디스크 공간 *: 10GB
- * SELinux *: 을 사용하지 않는 것이 좋습니다 "SELinux" 호스트.

  SELinux는 데이터 브로커 소프트웨어 업데이트를 차단하는 정책을 적용하고 데이터 브로커가 정상 작동에 필요한 엔드포인트에 접속하는 것을 차단할 수 있습니다.

네트워킹 요구 사항

- Linux 호스트에 소스와 타겟에 대한 접속이 있어야 합니다.
- 파일 서버는 Linux 호스트가 내보내기에 액세스할 수 있도록 허용해야 합니다.
- AWS로 나가는 트래픽을 위해 Linux 호스트에서 포트 443이 열려 있어야 합니다(데이터 브로커가 Amazon SQS 서비스와 지속적으로 통신).
- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

AWS에 대한 액세스 설정

S3 버킷을 포함하는 동기화 관계에 데이터 브로커를 사용할 계획이라면, AWS 액세스를 위한 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때는 프로그래밍 방식의 액세스와 특정 권한이 있는 AWS 사용자에게 AWS 키를 제공해야 합니다.

단계

1. 을 사용하여 IAM 정책을 생성합니다 "NetApp에서 제공하는 정책입니다"

   "AWS 지침을 확인하십시오"

2. 프로그래밍 방식으로 액세스할 수 있는 IAM 사용자를 생성합니다.

   "AWS 지침을 확인하십시오"

   데이터 브로커 소프트웨어를 설치할 때는 AWS 키를 지정해야 하므로 AWS 키를 반드시 복사해야 합니다.

Google Cloud에 대한 액세스를 활성화합니다

Google Cloud Storage 버킷을 포함하여 동기화 관계에 데이터 브로커를 사용할 계획이라면, Google Cloud 액세스를 위한 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 특정 권한이 있는 서비스 계정에 대한 키를 제공해야 합니다.

단계

1. 스토리지 관리자 권한이 없는 경우 Google Cloud 서비스 계정을 생성합니다.

2. JSON 형식으로 저장된 서비스 계정 키를 생성합니다.

   "Google Cloud 지침을 봅니다"

   파일에는 최소한 "project_id", "private_key" 및 "client_email" 속성이 포함되어야 합니다.

   ⓘ 키를 만들면 파일이 생성되어 컴퓨터에 다운로드됩니다.

3. JSON 파일을 Linux 호스트에 저장합니다.

Microsoft Azure에 대한 액세스 설정

Azure에 대한 액세스는 관계 동기화 마법사에서 스토리지 계정 및 연결 문자열을 제공하여 관계에 따라 정의됩니다.

데이터 브로커 설치

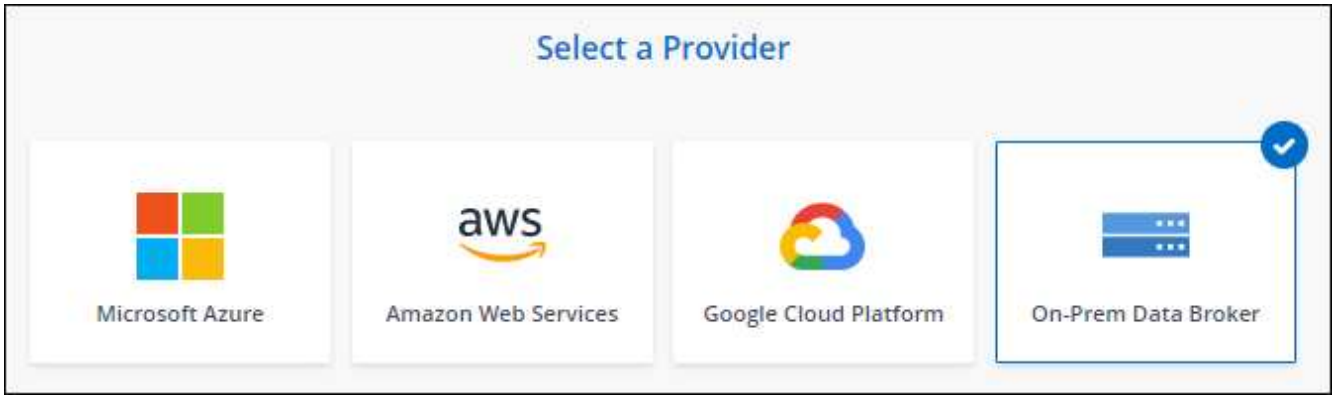
동기화 관계를 생성할 때 Linux 호스트에 데이터 브로커를 설치할 수 있습니다.

단계

1. 새 동기화 만들기 * 를 클릭합니다.
2. 동기화 관계 정의 * 페이지에서 소스 및 대상을 선택하고 * 계속 * 을 클릭합니다.

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 * 페이지에서 * 데이터 브로커 생성 * 을 클릭한 다음 * 온프레미스 데이터 브로커 * 를 선택합니다.



   ⓘ 옵션에 *_On-Premise_Data Broker * 라는 레이블이 표시되어 있지만 이 옵션은 온프레미스 또는 클라우드의 Linux 호스트에 적용됩니다.

4. 데이터 브로커의 이름을 입력하고 * 계속 * 을 클릭합니다.

   지침 페이지가 곧 로드됩니다. 설치 프로그램을 다운로드할 수 있는 고유 링크가 포함된 다음 지침을 따라야 합니다.

5. 지침 페이지에서 다음을 수행합니다.
   a. AWS *, * Google Cloud * 또는 둘 모두에 대한 액세스를 활성화할지 여부를 선택합니다.
   b. 설치 옵션 * 프록시 없음 *, * 프록시 서버 사용 * 또는 * 인증 프록시 서버 사용 * 을 선택합니다.

c. 명령을 사용하여 데이터 브로커를 다운로드하고 설치하십시오.

다음 단계에서는 가능한 각 설치 옵션에 대한 세부 정보를 제공합니다. 지침 페이지에 따라 설치 옵션에 따라 정확한 명령을 가져옵니다.

d. 설치 프로그램 다운로드:

- 프록시 없음:

'<URI>-o data_broker_installer.sh'라는 문구입니다

- 프록시 서버 사용:

'<URI>-o data_broker_installer.sh -x <proxy_host>:<proxy_port>'

- 인증 시 프록시 서버 사용:

'<URI>-o data_broker_installer.sh -x <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>'

URI입니다

Cloud Sync 설치 파일의 URI가 지침 페이지에 표시됩니다. 이 내용은 화면의 지시에 따라 온-프렘 데이터 브로커를 배포할 때 로드됩니다. 이 URI는 링크가 동적으로 생성되고 한 번만 사용할 수 있으므로 여기서 반복되지 않습니다. 다음 단계에 따라 Cloud Sync에서 URI를 가져옵니다.

e. 슈퍼유저로 전환하고 설치 프로그램을 실행 가능하게 만든 후 소프트웨어를 설치합니다.

아래 나열된 각 명령에는 AWS 액세스 및 Google Cloud 액세스에 대한 매개 변수가 포함되어 있습니다. 지침 페이지에 따라 설치 옵션에 따라 정확한 명령을 가져옵니다.

- 프록시 구성 없음:

'sudo -s chmod + x data_broker_installer.sh./data_broker_installer.sh -a <AWS_access_key> -s <AWS_secret_key> -g <absolute_path_to_the_json_file>'

- 프록시 구성:

sudo -s chmod + x data_broker_installer.sh. /data_broker_installer.sh -a <AWS_access_key> -s <AWS_secret_key> -g <absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>

- 인증이 있는 프록시 구성:

sudo -s chmod + x data_broker_installer.sh. /data_broker_installer.sh -a <AWS_access_key> -s <AWS_secret_key> -g <absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_username> -w <proxy_password>

AWS 키

사용자가 준비해야 하는 키입니다 다음 단계를 따릅니다. AWS 키는 데이터 브로커에 저장되며 사내 또는 클라우드 네트워크에서 실행됩니다. NetApp은 데이터 브로커 외에 다른 키는 사용하지 않습니다.

JSON 파일

미리 준비해야 하는 서비스 계정 키가 포함된 JSON 파일입니다 다음 단계를 따릅니다.

6. 데이터 브로커를 사용할 수 있게 되면 Cloud Sync에서 * 계속 * 을 클릭합니다.
7. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.