NetApp 복사 및 동기화 설명서

NetApp Copy and Sync

NetApp
October 06, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/data-services-copy-sync/index.html on October 06, 2025. Always check docs.netapp.com for the latest.

목차

NetApp 복사 및 동기화 설명서

릴리스 노트

NetApp Copy and Sync의 새로운 기능

NetApp Copy and Sync의 새로운 기능을 알아보세요.

2025년 10월 6일

BlueXP copy and sync 는 이제 **NetApp** 복사 및 동기화입니다**.**

BlueXP copy and sync NetApp 복사 및 동기화로 이름이 변경되었습니다.

BlueXP 는 이제 **NetApp** 콘솔입니다**.**

강화되고 재구성된 BlueXP 기반을 기반으로 구축된 NetApp 콘솔은 엔터프라이즈급 온프레미스 및 클라우드 환경 전반에서 NetApp 스토리지와 NetApp 데이터 서비스를 중앙에서 관리하여 실시간 통찰력, 더 빠른 워크플로, 간소화된 관리를 제공하며, 높은 보안성과 규정 준수를 보장합니다.

변경된 내용에 대한 자세한 내용은 다음을 참조하세요."NetApp 콘솔 릴리스 노트" .

2025년 2월 2일

데이터 브로커를 위한 새로운 **OS** 지원

데이터 브로커는 이제 Red Hat Enterprise 9.4, Ubuntu 23.04, Ubuntu 24.04를 실행하는 호스트에서 지원됩니다.

"Linux 호스트 요구 사항 보기" .

2024년 10월 27일

버그 수정

NetApp Copy and Sync와 데이터 브로커를 업데이트하여 몇 가지 버그를 수정했습니다. 새로운 데이터 브로커 버전은 1.0.56입니다.

2024년 9월 16일

버그 수정

NetApp Copy and Sync와 데이터 브로커를 업데이트하여 몇 가지 버그를 수정했습니다. 새로운 데이터 브로커 버전은 1.0.55입니다.

2024년 8월 11일

버그 수정

NetApp Copy and Sync와 데이터 브로커를 업데이트하여 몇 가지 버그를 수정했습니다. 새로운 데이터 브로커 버전은 1.0.54입니다.

2024년 7월 14일

버그 수정

몇 가지 버그를 수정하기 위해 Copy and Sync와 데이터 브로커를 업데이트했습니다. 새로운 데이터 브로커 버전은 1.0.53입니다.

2024년 6월 2일

버그 수정

NetApp Copy and Sync가 업데이트되어 몇 가지 버그가 수정되었습니다. 데이터 브로커도 보안 업데이트를 적용하도록 업데이트되었습니다. 새로운 데이터 브로커 버전은 1.0.52입니다.

2024년 4월 8일

RHEL 8.9 지원

데이터 브로커는 이제 Red Hat Enterprise Linux 8.9를 실행하는 호스트에서 지원됩니다.

"Linux 호스트 요구 사항 보기" .

2024년 2월 11일

정규식으로 디렉토리 필터링

이제 사용자는 정규식을 사용하여 디렉토리를 필터링할 수 있습니다.

"디렉토리 제외 기능에 대해 자세히 알아보세요."

2023년 11월 26일

Azure Blob에 대한 콜드 스토리지 클래스 지원

이제 동기화 관계를 만들 때 콜드 스토리지 Azure Blob 계층을 사용할 수 있습니다.

"동기화 관계 생성에 대해 자세히 알아보세요."

AWS 데이터 브로커에서 텔아비브 지역 지원

이제 AWS에서 데이터 브로커를 생성할 때 텔아비브가 지원되는 지역이 되었습니다.

"AWS에서 데이터 브로커를 만드는 방법에 대해 자세히 알아보세요" .

데이터 브로커를 위한 노드 버전 업데이트

모든 새로운 데이터 브로커는 이제 노드 버전 21.2.0을 사용합니다. CentOS 7.0 및 Ubuntu Server 18.0과 같이 이 업데이트와 호환되지 않는 데이터 브로커는 더 이상 NetApp Copy and Sync와 함께 작동하지 않습니다.

2023년 9월 3일

정규식으로 파일 제외

이제 사용자는 정규식을 사용하여 파일을 제외할 수 있습니다.

"파일 확장자 제외 기능에 대해 자세히 알아보세요."

Azure 데이터 브로커를 생성할 때 **S3** 키 추가

이제 사용자는 Azure 데이터 브로커를 생성할 때 AWS S3 액세스 키와 비밀 키를 추가할 수 있습니다.

"Azure에서 데이터 브로커를 만드는 방법에 대해 자세히 알아보세요."

2023년 8월 6일

데이터 브로커를 만들 때 기존 **Azure** 보안 그룹을 사용하세요**.**

이제 사용자는 데이터 브로커를 만들 때 기존 Azure 보안 그룹을 사용할 수 있습니다.

데이터 브로커를 생성할 때 사용되는 서비스 계정에는 다음과 같은 권한이 있어야 합니다.

- "Microsoft.Network/networkSecurityGroups/securityRules/read"
- "Microsoft.Network/networkSecurityGroups/read"

"Azure에서 데이터 브로커를 만드는 방법에 대해 자세히 알아보세요."

Google Storage와 동기화할 때 데이터 암호화

이제 사용자는 Google Storage 버킷을 대상으로 동기화 관계를 생성할 때 고객 관리 암호화 키를 지정할 수 있습니다. 키를 직접 입력하거나 단일 지역의 키 목록에서 선택할 수 있습니다.

데이터 브로커를 생성할 때 사용되는 서비스 계정에는 다음과 같은 권한이 있어야 합니다.

- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list

"Google Cloud Storage 버킷 요구 사항에 대해 자세히 알아보세요."

2023년 7월 9일

여러 동기화 관계를 한 번에 제거

이제 사용자는 UI에서 한 번에 두 개 이상의 동기화 관계를 삭제할 수 있습니다.

"동기화 관계 삭제에 대해 자세히 알아보세요."

ACL만 복사

이제 사용자는 CIF 및 NFS 관계에서 ACL 정보를 복사하기 위한 추가 옵션을 사용할 수 있습니다. 동기화 관계를 만들거나 관리할 때 파일만 복사하거나, ACL 정보만 복사하거나, 파일과 ACL 정보를 복사할 수 있습니다.

"ACL 복사에 대해 자세히 알아보세요."

Node.js 20으로 업데이트되었습니다**.**

Copy and Sync가 Node.js 20으로 업데이트되었습니다. 사용 가능한 모든 데이터 브로커가 업데이트됩니다. 이 업데이트와 호환되지 않는 운영 체제는 설치할 수 없으며, 호환되지 않는 기존 시스템에서는 성능 문제가 발생할 수 있습니다.

2023년 6월 11일

분 단위로 자동 중단 지원

완료되지 않은 활성 동기화는 이제 동기화 시간 초과 기능을 사용하여 15분 후에 중단할 수 있습니다.

"동기화 시간 초과 설정에 대해 자세히 알아보세요" .

액세스 시간 메타데이터 복사

파일 시스템을 포함하는 관계에서 객체 복사 기능은 이제 액세스 시간 메타데이터를 복사합니다.

"개체 복사 설정에 대해 자세히 알아보세요" .

2023년 5월 8일

하드 링크 기능

이제 사용자는 보안되지 않은 NFS 간 관계를 포함하는 동기화에 하드 링크를 포함할 수 있습니다.

"파일 유형 설정에 대해 자세히 알아보세요" .

보안 **NFS** 관계에서 데이터 브로커에 대한 사용자 인증서를 추가하는 기능

이제 사용자는 보안 NFS 관계를 생성할 때 대상 데이터 브로커에 대한 자체 인증서를 설정할 수 있습니다. 그렇게 하려면 서버 이름을 설정하고 개인 키와 인증서 ID를 제공해야 합니다. 이 기능은 모든 데이터 브로커에서 사용할 수 있습니다.

최근 수정된 파일에 대한 확장된 제외 기간

이제 사용자는 예약된 동기화보다 최대 365일 전에 수정된 파일을 제외할 수 있습니다.

"최근 수정된 파일 설정에 대해 자세히 알아보세요" .

UI에서 관계 **ID**로 관계 필터링

RESTful API를 사용하는 사용자는 이제 관계 ID를 사용하여 관계를 필터링할 수 있습니다.

"NetApp Copy and Sync에서 RESTful API를 사용하는 방법에 대해 자세히 알아보세요." .

"제외 디렉터리 설정에 대해 자세히 알아보세요" .

2023년 4월 2일

Azure Data Lake Storage Gen2 관계에 대한 추가 지원

이제 다음을 사용하여 Azure Data Lake Storage Gen2를 소스 및 대상으로 동기화 관계를 만들 수 있습니다.

- Azure NetApp Files
- ONTAP 용 Amazon FSx
- Cloud Volumes ONTAP
- 온프레미스 ONTAP

"지원되는 동기화 관계에 대해 자세히 알아보세요." .

전체 경로로 디렉토리 필터링

이름으로 디렉토리를 필터링하는 것 외에도 이제 전체 경로로 디렉토리를 필터링할 수 있습니다.

"제외 디렉터리 설정에 대해 자세히 알아보세요" .

2023년 3월 7일

AWS 데이터 브로커를 위한 **EBS** 암호화

이제 계정의 KMS 키를 사용하여 AWS 데이터 브로커 볼륨을 암호화할 수 있습니다.

"AWS에서 데이터 브로커를 만드는 방법에 대해 자세히 알아보세요" .

2023년 2월 5일

Azure Data Lake Storage Gen2, ONTAP S3 Storage 및 **NFS**에 대한 추가 지원

Cloud Sync 이제 ONTAP S3 스토리지 및 NFS에 대한 추가 동기화 관계를 지원합니다.

- ONTAP S3 스토리지에서 NFS로
- NFS에서 ONTAP S3 스토리지로

Cloud Sync 다음을 위한 소스 및 대상으로 Azure Data Lake Storage Gen2에 대한 추가 지원도 제공합니다.

- NFS 서버
- SMB 서버
- ONTAP S3 스토리지
- StorageGRID
- IBM 클라우드 객체 스토리지

"지원되는 동기화 관계에 대해 자세히 알아보세요." .

Amazon Web Services 데이터 브로커 운영 체제로 업그레이드

AWS 데이터 브로커의 운영 체제가 Amazon Linux 2022로 업그레이드되었습니다.

"AWS의 데이터 브로커 인스턴스에 대해 자세히 알아보세요" .

2023년 1월 3일

UI에 데이터 브로커 로컬 구성 표시

이제 사용자가 UI에서 각 데이터 브로커의 로컬 구성을 볼 수 있는 구성 표시 옵션이 있습니다.

"데이터 브로커 그룹 관리에 대해 자세히 알아보세요" .

Azure 및 **Google Cloud** 데이터 브로커 운영 체제로 업그레이드

Azure와 Google Cloud의 데이터 브로커 운영 체제가 Rocky Linux 9.0으로 업그레이드되었습니다.

"Azure의 데이터 브로커 인스턴스에 대해 자세히 알아보세요." .

"Google Cloud의 데이터 브로커 인스턴스에 대해 자세히 알아보세요." .

2022년 12월 11일

이름으로 디렉토리 필터링

동기화 관계에 대해 새로운 디렉토리 이름 제외 설정을 사용할 수 있습니다. 사용자는 동기화에서 최대 15개의 디렉토리 이름을 필터링할 수 있습니다. .copy-offload, .snapshot, ~snapshot 디렉토리는 기본적으로 제외됩니다.

"디렉터리 이름 제외 설정에 대해 자세히 알아보세요." .

추가 **Amazon S3** 및 **ONTAP S3** 스토리지 지원

Cloud Sync 이제 AWS S3 및 ONTAP S3 스토리지에 대한 추가 동기화 관계를 지원합니다.

- AWS S3에서 ONTAP S3 스토리지로
- ONTAP S3 스토리지에서 AWS S3로

"지원되는 동기화 관계에 대해 자세히 알아보세요." .

2022년 10월 30일

Microsoft Azure에서 지속적인 동기화

이제 Azure 데이터 브로커를 사용하여 원본 Azure 저장소 버킷에서 클라우드 저장소로의 지속적인 동기화 설정이 지원됩니다.

초기 데이터 동기화 후, Cloud Sync 소스 Azure 스토리지 버킷의 변경 사항을 수신하고 발생하는 모든 변경 사항을 대상에 지속적으로 동기화합니다. 이 설정은 Azure 스토리지 버킷에서 Azure Blob 스토리지, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS 및 StorageGRID 로 동기화할 때 사용할 수 있습니다.

Azure 데이터 브로커에는 이 설정을 사용하려면 사용자 지정 역할과 다음 권한이 필요합니다.

```
'Microsoft.Storage/storageAccounts/read',
'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',
'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',
'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete',
'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action',
'Microsoft.EventGrid/systemTopics/read',
'Microsoft.EventGrid/systemTopics/write',
'Microsoft.EventGrid/systemTopics/delete',
'Microsoft.EventGrid/eventSubscriptions/write',
'Microsoft.Storage/storageAccounts/write'
```

"연속 동기화 설정에 대해 자세히 알아보세요" .

2022년 9월 4일

추가 **Google** 드라이브 지원

- Cloud Sync 이제 Google Drive에 대한 추가 동기화 관계를 지원합니다.
  - Google Drive에서 NFS 서버로
  - Google Drive에서 SMB 서버로
- Google Drive를 포함한 동기화 관계에 대한 보고서를 생성할 수도 있습니다.

  "보고서에 대해 자세히 알아보세요" .

지속적인 동기화 향상

이제 다음 유형의 동기화 관계에서 지속적인 동기화 설정을 활성화할 수 있습니다.

- S3 버킷에서 NFS 서버로
- Google Cloud Storage를 NFS 서버로

"연속 동기화 설정에 대해 자세히 알아보세요" .

이메일 알림

이제 이메일로 Cloud Sync 알림을 받을 수 있습니다.

이메일로 알림을 받으려면 동기화 관계에서 알림 설정을 활성화한 다음 NetApp 콘솔에서 알림 및 알림 설정을 구성해야 합니다.

"알림 설정 방법 알아보기" .

2022년 7월 31일

구글 드라이브

이제 NFS 서버나 SMB 서버의 데이터를 Google Drive에 동기화할 수 있습니다. "내 드라이브"와 "공유 드라이브"는 모두 대상으로 지원됩니다.

Google Drive를 포함하는 동기화 관계를 만들려면 먼저 필요한 권한과 개인 키가 있는 서비스 계정을 설정해야 합니다. "Google Drive 요구 사항에 대해 자세히 알아보세요" .

"지원되는 동기화 관계 목록 보기" .

추가 **Azure Data Lake** 지원

Cloud Sync 이제 Azure Data Lake Storage Gen2에 대한 추가 동기화 관계를 지원합니다.

- Amazon S3에서 Azure Data Lake Storage Gen2로
- IBM Cloud Object Storage에서 Azure Data Lake Storage Gen2로
- StorageGRID 에서 Azure Data Lake Storage Gen2로

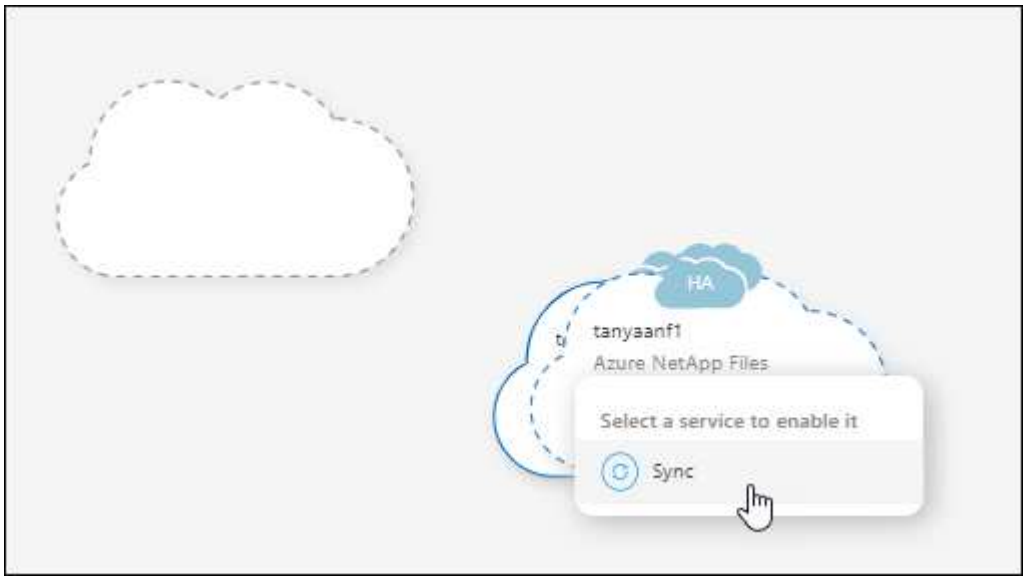
"지원되는 동기화 관계 목록 보기" .

동기화 관계를 설정하는 새로운 방법

NetApp 콘솔의 시스템 페이지에서 직접 동기화 관계를 설정하는 추가 방법을 추가했습니다.

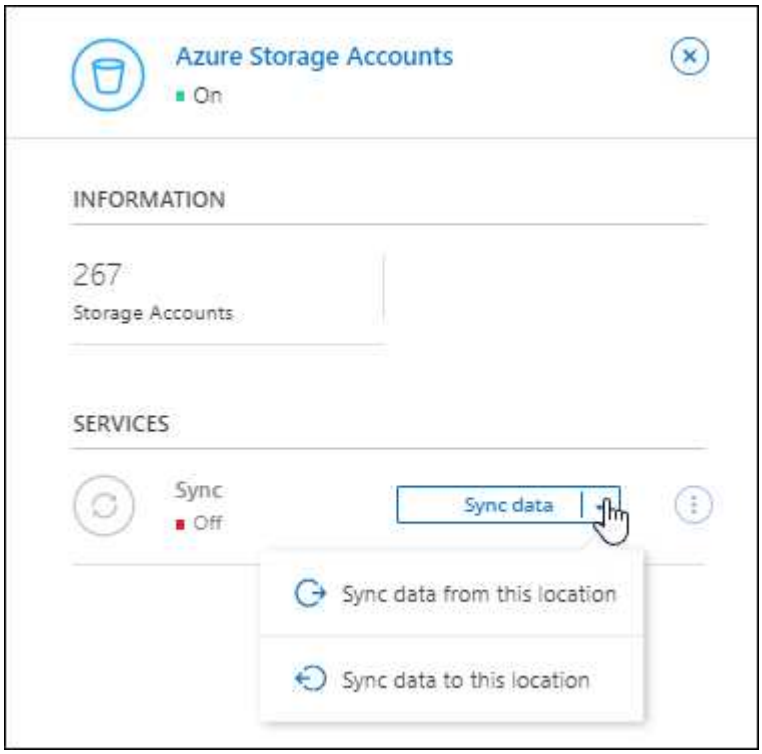
드래그 앤 드롭

이제 시스템 페이지에서 한 시스템을 다른 시스템 위로 끌어다 놓아 동기화 관계를 설정할 수 있습니다.



오른쪽 패널 설정

이제 시스템 페이지에서 시스템을 선택한 다음 오른쪽 패널에서 동기화 옵션을 선택하여 Azure Blob 저장소 또는 Google Cloud Storage에 대한 동기화 관계를 설정할 수 있습니다.



2022년 7월 3일

Azure Data Lake Storage Gen2 지원

이제 NFS 서버 또는 SMB 서버에서 Azure Data Lake Storage Gen2로 데이터를 동기화할 수 있습니다.

Azure Data Lake를 포함하는 동기화 관계를 만들 때는 Cloud Sync 에 스토리지 계정 연결 문자열을 제공해야 합니다. SAS(공유 액세스 서명)가 아닌 일반 연결 문자열이어야 합니다.

"지원되는 동기화 관계 목록 보기" .

Google Cloud Storage에서 지속적인 동기화

이제 소스 Google Cloud Storage 버킷에서 클라우드 스토리지 대상으로의 연속 동기화 설정이 지원됩니다.

초기 데이터 동기화 후, Cloud Sync 소스 Google Cloud Storage 버킷의 변경 사항을 수신하고 발생하는 모든 변경 사항을 대상에 지속적으로 동기화합니다. 이 설정은 Google Cloud Storage 버킷에서 S3, Google Cloud Storage, Azure Blob Storage, StorageGRID 또는 IBM Storage로 동기화할 때 사용할 수 있습니다.

이 설정을 사용하려면 데이터 브로커에 연결된 서비스 계정에는 다음 권한이 필요합니다.

```
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
```

"연속 동기화 설정에 대해 자세히 알아보세요" .

새로운 **Google Cloud** 지역 지원

Cloud Sync 데이터 브로커는 이제 다음 Google Cloud 지역에서 지원됩니다.

- 콜럼버스(us-east5)
- 댈러스(us-south1)
- 마드리드(유럽-남서1)
- 밀라노(europe-west8)
- 파리(europe-west9)

새로운 **Google Cloud** 머신 유형

Google Cloud의 데이터 브로커에 대한 기본 머신 유형은 이제 n2-standard-4입니다.

2022년 6월 6일

연속 동기화

새로운 설정을 사용하면 소스 S3 버킷의 변경 사항을 대상에 지속적으로 동기화할 수 있습니다.

초기 데이터 동기화 후, Cloud Sync 소스 S3 버킷의 변경 사항을 수신하고 발생하는 모든 변경 사항을 대상에 지속적으로 동기화합니다. 예약된 간격으로 소스를 다시 스캔할 필요가 없습니다. 이 설정은 S3 버킷에서 S3, Google Cloud Storage, Azure Blob Storage, StorageGRID 또는 IBM Storage로 동기화할 때만 사용할 수 있습니다.

이 설정을 사용하려면 데이터 브로커와 연결된 IAM 역할에 다음 권한이 필요합니다.

```
"s3:GetBucketNotification",
"s3:PutBucketNotification"
```

이러한 권한은 새로 만든 모든 데이터 브로커에 자동으로 추가됩니다.

"연속 동기화 설정에 대해 자세히 알아보세요" .

모든 **ONTAP** 볼륨 표시

동기화 관계를 만들면 이제 Cloud Sync 에서 소스 Cloud Volumes ONTAP 시스템, 온프레미스 ONTAP 클러스터 또는 FSx for ONTAP 파일 시스템의 모든 볼륨이 표시됩니다.

이전에는 Cloud Sync 선택한 프로토콜과 일치하는 볼륨만 표시했습니다. 이제 모든 볼륨이 표시되지만, 선택한 프로토콜과 일치하지 않거나 공유 또는 내보내기가 없는 볼륨은 회색으로 표시되어 선택할 수 없습니다.

Azure Blob에 태그 복사

Azure Blob이 대상인 동기화 관계를 만들면 이제 Cloud Sync 하여 태그를 Azure Blob 컨테이너에 복사할 수 있습니다.

- 설정 페이지에서 개체 복사 설정을 사용하여 소스에서 Azure Blob 컨테이너로 태그를 복사할 수 있습니다. 이는 메타데이터를 복사하는 것에 추가됩니다.
- 태그/메타데이터 페이지에서 Azure Blob 컨테이너에 복사되는 개체에 설정할 Blob 인덱스 태그를 지정할 수 있습니다. 이전에는 관계 메타데이터만 지정할 수 있었습니다.

이러한 옵션은 Azure Blob이 대상이고 소스가 Azure Blob이거나 S3 호환 엔드포인트(S3, StorageGRID 또는 IBM Cloud Object Storage)인 경우 지원됩니다.

2022년 5월 1일

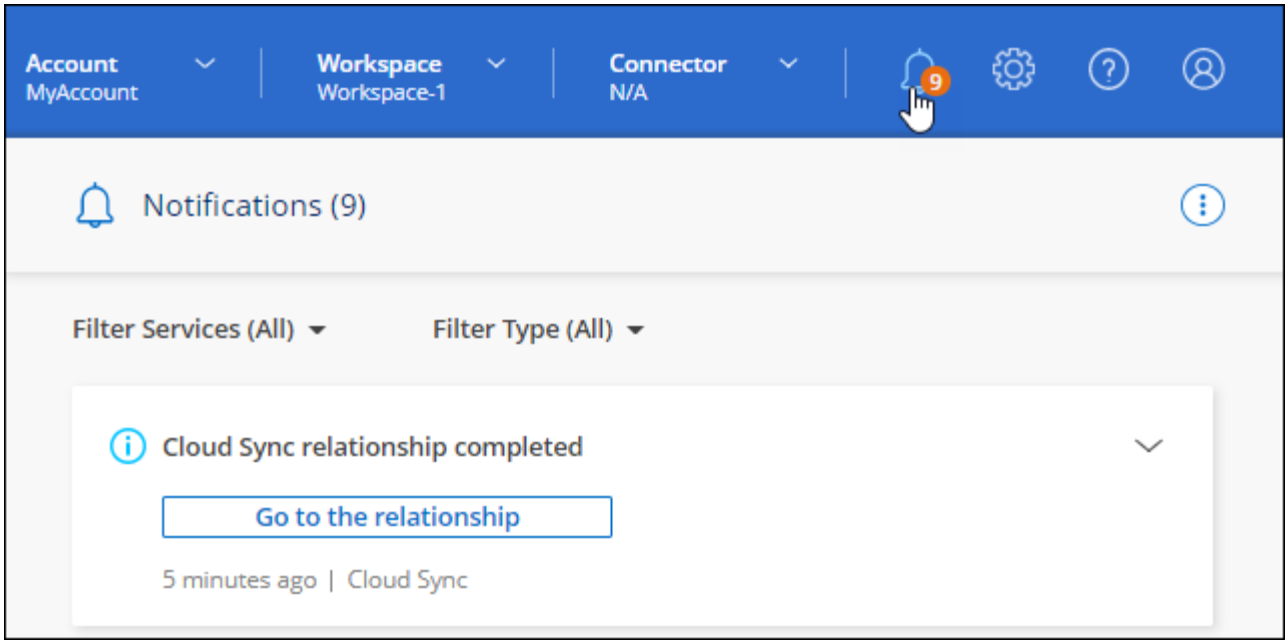
동기화 시간 초과

동기화 관계에 대한 새로운 동기화 시간 초과 설정을 사용할 수 있습니다. 이 설정을 사용하면 지정된 시간 또는 일 수 동안 동기화가 완료되지 않을 경우 Cloud Sync 데이터 동기화를 취소할지 여부를 정의할 수 있습니다.

"동기화 관계 설정 변경에 대해 자세히 알아보세요." .

알림

동기화 관계에 대한 새로운 알림 설정을 사용할 수 있습니다. 이 설정을 사용하면 NetApp 콘솔의 알림 센터에서 Cloud Sync 알림을 받을지 여부를 선택할 수 있습니다. 성공적인 데이터 동기화, 실패한 데이터 동기화, 취소된 데이터 동기화에 대한 알림을 활성화할 수 있습니다.



"동기화 관계 설정 변경에 대해 자세히 알아보세요." .

2022년 4월 3일

데이터 브로커 그룹 개선

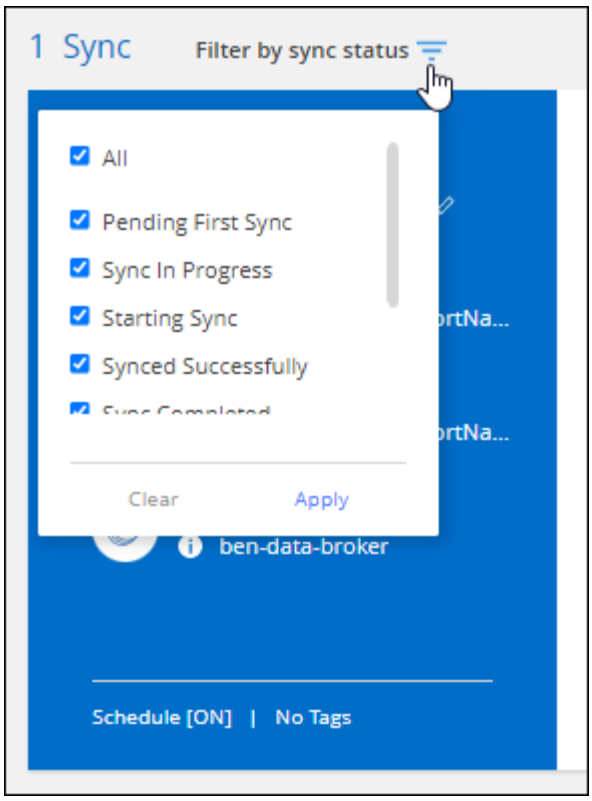
데이터 브로커 그룹에 여러 가지 개선 사항을 적용했습니다.

- 이제 데이터 브로커를 새 그룹이나 기존 그룹으로 이동할 수 있습니다.
- 이제 데이터 브로커의 프록시 구성을 업데이트할 수 있습니다.
- 마지막으로 데이터 브로커 그룹을 삭제할 수도 있습니다.

"데이터 브로커 그룹을 관리하는 방법을 알아보세요" .

대시보드 필터

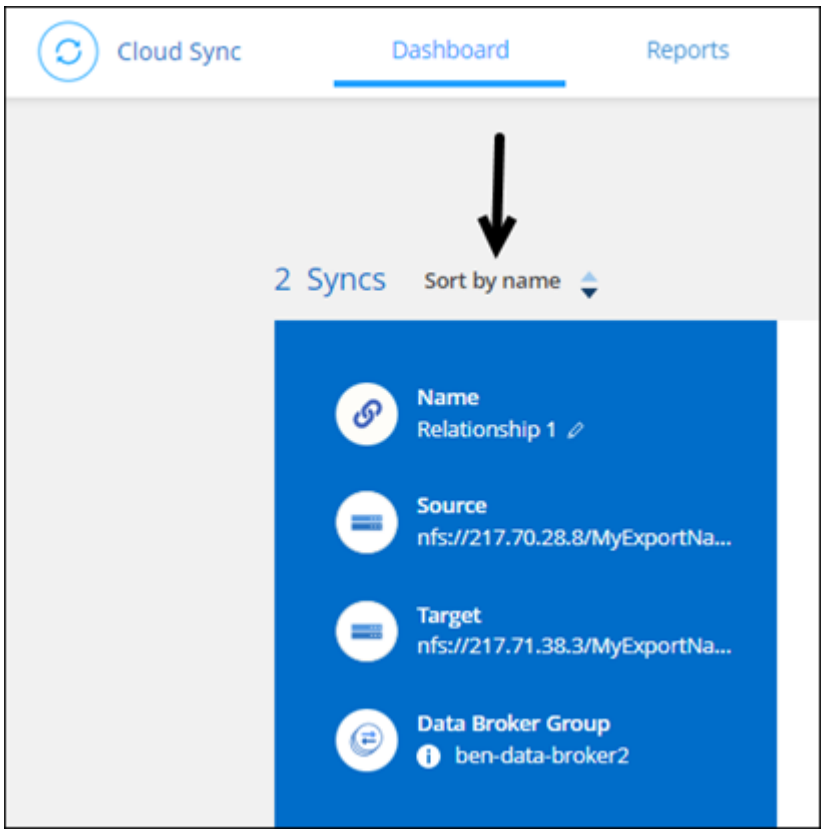
이제 동기화 대시보드의 내용을 필터링하여 특정 상태와 일치하는 동기화 관계를 더 쉽게 찾을 수 있습니다. 예를 들어, 실패 상태인 동기화 관계를 필터링할 수 있습니다.



2022년 3월 3일

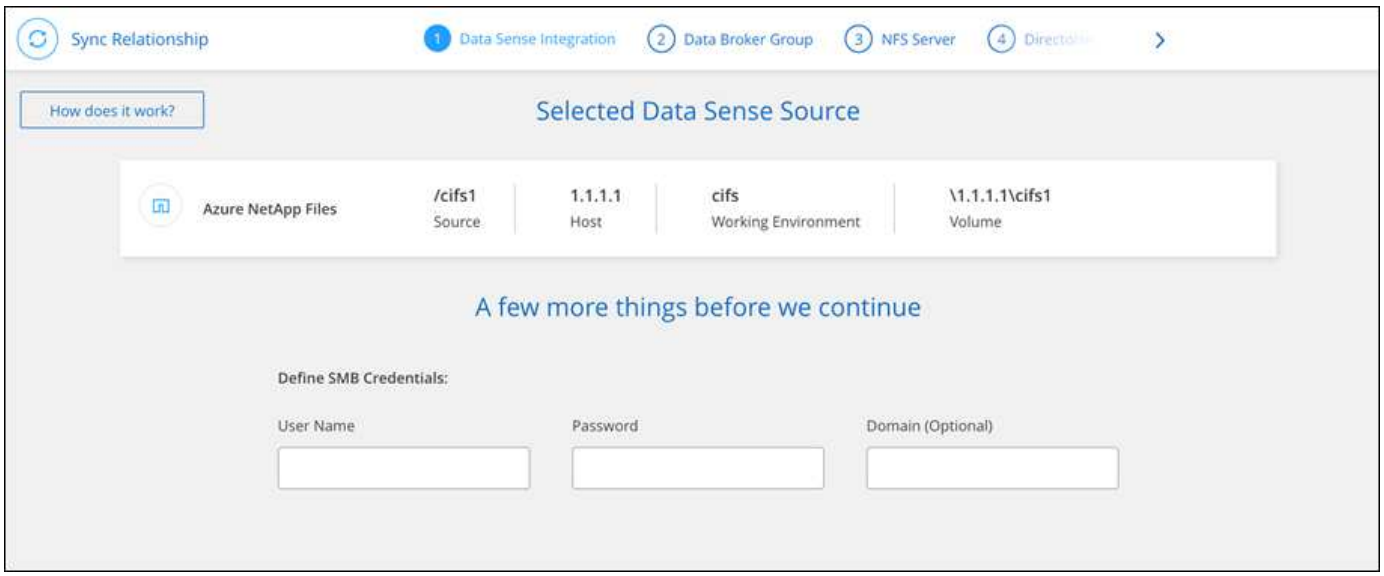
대시보드에서 정렬

이제 대시보드를 동기화 관계 이름별로 정렬합니다.



데이터 감지 통합 향상

이전 릴리스에서는 Cloud Data Sense와 Cloud Sync 통합을 도입했습니다. 이번 업데이트에서는 동기화 관계를 더 쉽게 만들 수 있도록 통합을 강화했습니다. Cloud Data Sense에서 데이터 동기화를 시작하면 모든 소스 정보가 단일 단계에 포함되므로 몇 가지 주요 세부 정보만 입력하면 됩니다.

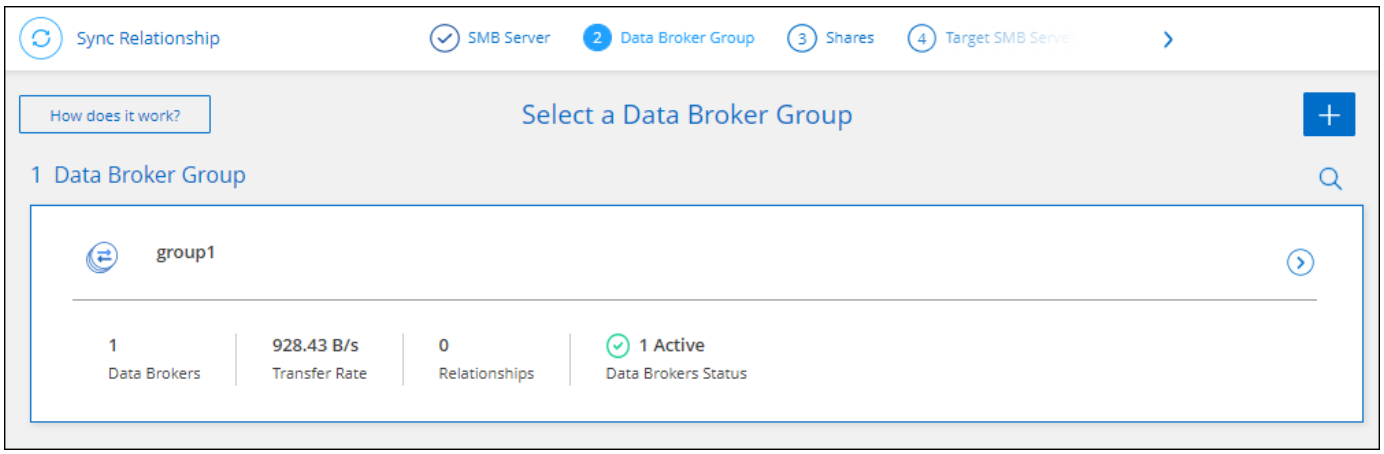


2022년 2월 6일

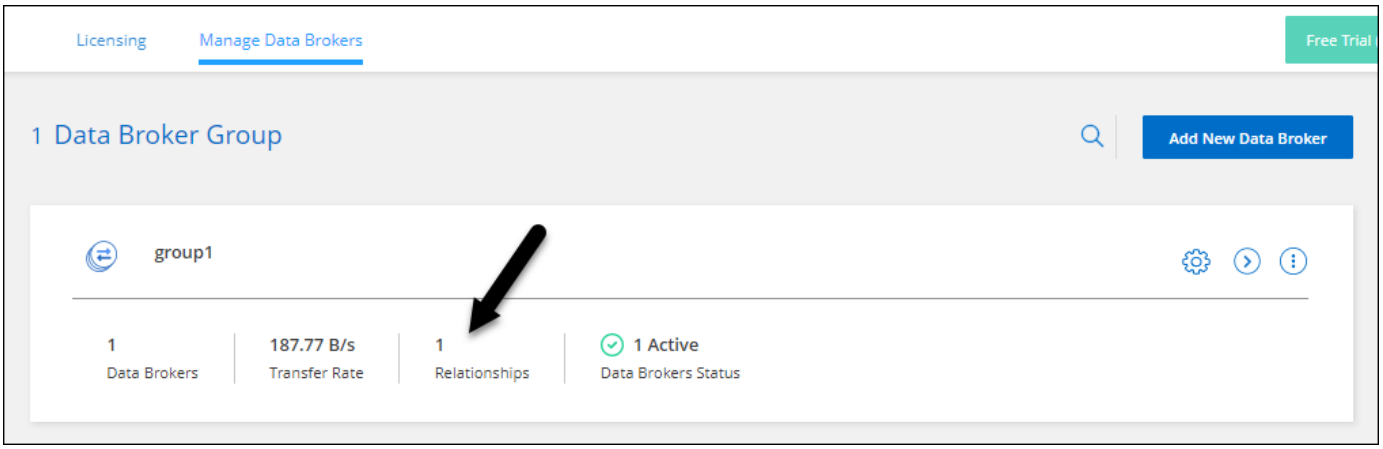
데이터 브로커 그룹 강화

데이터 브로커 그룹을 강조하여 데이터 브로커와의 상호 작용 방식을 변경했습니다.

예를 들어, 새로운 동기화 관계를 만들 때 특정 데이터 브로커를 선택하는 대신, 관계에 사용할 데이터 브로커 _그룹_을 선택합니다.



데이터 브로커 관리 탭에서는 데이터 브로커 그룹이 관리하는 동기화 관계의 수도 표시됩니다.



PDF 보고서 다운로드

이제 보고서 PDF를 다운로드할 수 있습니다.

"보고서에 대해 자세히 알아보세요" .

2022년 1월 2일

새로운 **Box** 동기화 관계

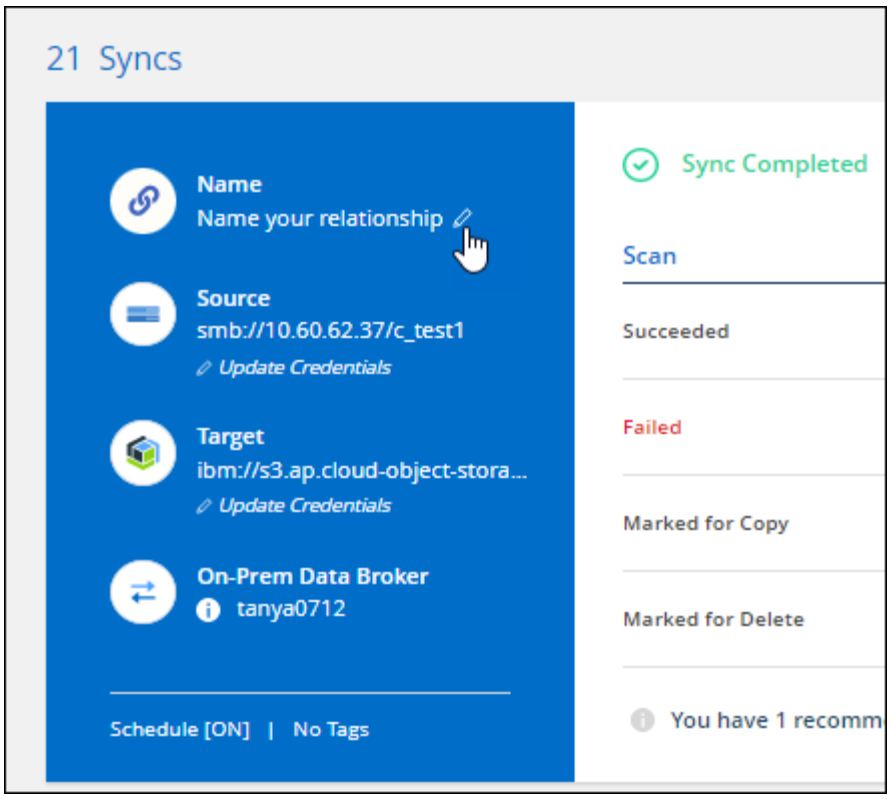
두 가지 새로운 동기화 관계가 지원됩니다.

- Box에서 Azure NetApp Files
- ONTAP 용 Amazon FSx 로 박스 전송

"지원되는 동기화 관계 목록 보기" .

관계 이름

이제 각 동기화 관계에 의미 있는 이름을 지정하여 각 관계의 목적을 더 쉽게 식별할 수 있습니다. 관계를 생성할 때 이름을 추가할 수 있으며, 이후 언제든지 추가할 수 있습니다.



S3 개인 링크

Amazon S3에서 데이터를 동기화할 때 S3 개인 링크를 사용할지 여부를 선택할 수 있습니다. 데이터 브로커가 소스에서 타겟으로 데이터를 복사할 때는 개인 링크를 거칩니다.

이 기능을 사용하려면 데이터 브로커와 연결된 IAM 역할에 다음과 같은 권한이 필요합니다.

```
"ec2:DescribeVpcEndpoints"
```

이 권한은 새로 만든 모든 데이터 브로커에 자동으로 추가됩니다.

빙하 즉시 검색

이제 Amazon S3가 동기화 관계의 대상인 경우 *Glacier Instant Retrieval* 스토리지 클래스를 선택할 수 있습니다.

개체 스토리지에서 **SMB** 공유로의 **ACL**

이제 Cloud Sync 개체 스토리지의 ACL을 SMB 공유로 복사하는 기능을 지원합니다. 이전에는 SMB 공유에서 개체 스토리지로 ACL을 복사하는 것만 지원했습니다.

SFTP에서 **S3**로

SFTP에서 Amazon S3로 동기화 관계를 만드는 기능이 이제 사용자 인터페이스에서 지원됩니다. 이 동기화 관계는 이전에는 API로만 지원되었습니다.

테이블 뷰 향상

대시보드의 테이블 보기를 사용 편의성을 위해 새롭게 디자인했습니다. *추가 정보*를 선택하면 Cloud Sync 대시보드를 필터링하여 해당 관계에 대한 자세한 정보를 표시합니다.

자카르타 지역 지원

이제 Cloud Sync AWS 아시아 태평양(자카르타) 지역에 데이터 브로커를 배포하는 것을 지원합니다.

2021년 11월 28일

SMB에서 개체 스토리지로의 **ACL**

이제 Cloud Sync 소스 SMB 공유에서 개체 스토리지로 동기화 관계를 설정할 때 액세스 제어 목록(ACL)을 복사할 수 있습니다(ONTAP S3 제외).

Cloud Sync 개체 스토리지에서 SMB 공유로 ACL을 복사하는 것을 지원하지 않습니다.

"SMB 공유에서 ACL을 복사하는 방법을 알아보세요" .

라이센스 업데이트

이제 연장한 Cloud Sync 라이선스를 업데이트할 수 있습니다.

NetApp 에서 구매한 Cloud Sync 라이선스를 연장한 경우 라이선스를 다시 추가하여 만료 날짜를 새로 고칠 수 있습니다.

"라이센스를 업데이트하는 방법을 알아보세요" .

Box 자격 증명 업데이트

이제 기존 동기화 관계에 대한 Box 자격 증명을 업데이트할 수 있습니다.

"자격 증명을 업데이트하는 방법을 알아보세요" .

2021년 10월 31일

박스 지지대

Box 지원은 이제 Cloud Sync 사용자 인터페이스에서 미리 보기로 제공됩니다.

상자는 여러 유형의 동기화 관계에서 소스 또는 대상이 될 수 있습니다. "지원되는 동기화 관계 목록 보기" .

생성 날짜 설정

SMB 서버가 소스인 경우 _생성 날짜_라는 새로운 동기화 관계 설정을 사용하면 특정 날짜 이후, 특정 날짜 이전 또는 특정 기간 사이에 생성된 파일을 동기화할 수 있습니다.

"Cloud Sync 설정에 대해 자세히 알아보세요" .

2021년 10월 4일

추가 **Box** 지원

Cloud Sync 이제 추가 동기화 관계를 지원합니다. "상자" Cloud Sync API를 사용할 때:

- Amazon S3에서 Box로
- IBM Cloud Object Storage에서 Box로
- StorageGRID 에서 Box로
- NFS 서버로의 박스
- SMB 서버로의 박스

"API를 사용하여 동기화 관계를 설정하는 방법을 알아보세요." .

SFTP 경로에 대한 보고서

이제 할 수 있습니다"보고서를 만들다" SFTP 경로의 경우.

2021년 9월 2일

ONTAP 용 **FSx** 지원

이제 Amazon FSx for ONTAP 파일 시스템에서 데이터를 동기화할 수 있습니다.

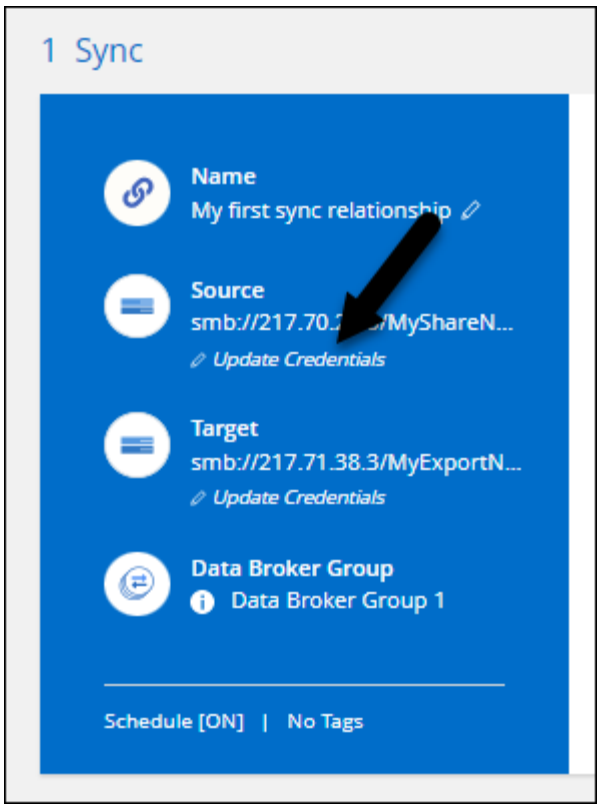
- "Amazon FSx for ONTAP 에 대해 알아보세요"
- "지원되는 동기화 관계 보기"
- "Amazon FSx for ONTAP 에 대한 동기화 관계를 만드는 방법을 알아보세요."

2021년 8월 1일

자격 증명 업데이트

이제 Cloud Sync 사용하면 기존 동기화 관계의 소스 또는 대상의 최신 자격 증명으로 데이터 브로커를 업데이트할 수 있습니다.

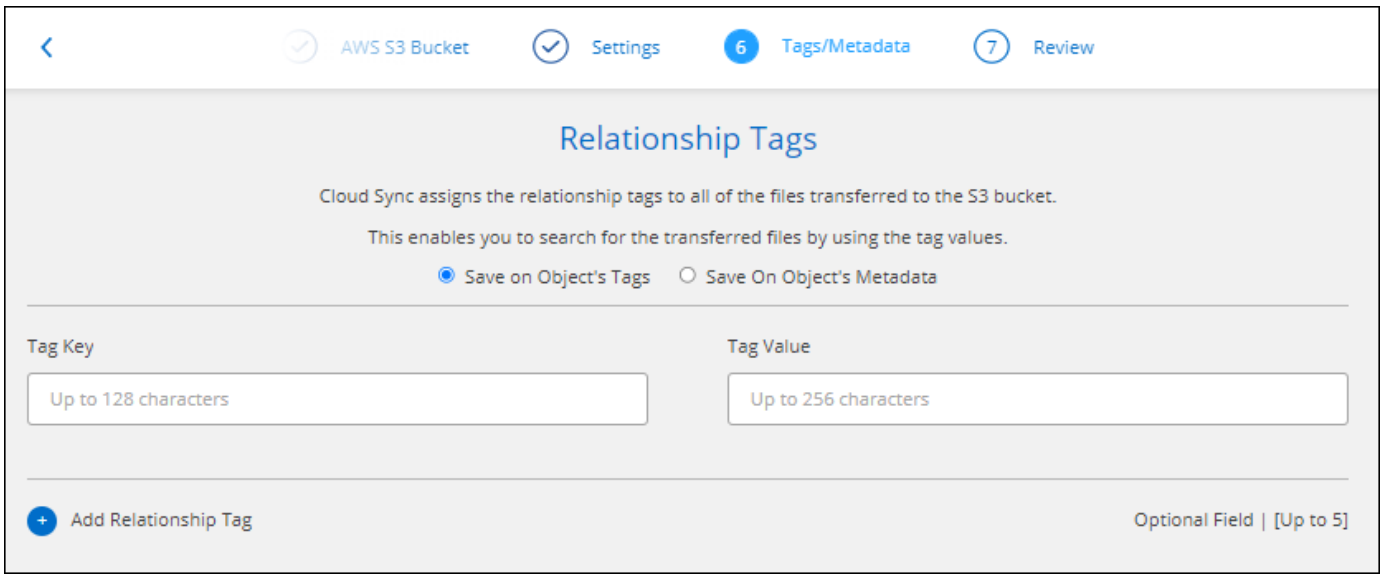
보안 정책에 따라 주기적으로 자격 증명을 업데이트해야 하는 경우 이러한 향상 기능이 도움이 될 수 있습니다. "자격 증명을 업데이트하는 방법을 알아보세요" .



객체 스토리지 대상에 대한 태그

동기화 관계를 생성할 때 이제 동기화 관계의 개체 스토리지 대상에 태그를 추가할 수 있습니다.

태그 추가는 Amazon S3, Azure Blob, Google Cloud Storage, IBM Cloud Object Storage 및 StorageGRID 에서 지원됩니다.



Box 지원

이제 Cloud Sync 지원됩니다. "상자" Cloud Sync API를 사용할 때 Amazon S3, StorageGRID 및 IBM Cloud Object Storage에 대한 동기화 관계의 소스로 사용됩니다.

"API를 사용하여 동기화 관계를 설정하는 방법을 알아보세요." .

Google Cloud의 데이터 브로커를 위한 공용 **IP**

Google Cloud에 데이터 브로커를 배포할 때 이제 가상 머신 인스턴스에 대한 공용 IP 주소를 활성화할지 비활성화할지 선택할 수 있습니다.

"Google Cloud에서 데이터 브로커를 배포하는 방법을 알아보세요." .

Azure NetApp Files 용 이중 프로토콜 볼륨

Azure NetApp Files 대한 소스 또는 대상 볼륨을 선택하면 이제 Cloud Sync 동기화 관계에 대해 선택한 프로토콜에 관계없이 이중 프로토콜 볼륨이 표시됩니다.

2021년 7월 7일

ONTAP S3 스토리지 및 **Google Cloud Storage**

Cloud Sync 이제 사용자 인터페이스에서 ONTAP S3 Storage와 Google Cloud Storage 버킷 간의 동기화 관계를 지원합니다.

"지원되는 동기화 관계 목록 보기" .

객체 메타데이터 태그

이제 동기화 관계를 생성하고 설정을 활성화하면 Cloud Sync 개체 기반 저장소 간에 개체 메타데이터와 태그를 복사할 수 있습니다.

"개체 복사 설정에 대해 자세히 알아보세요" .

HashiCorp Vault 지원

이제 Google Cloud 서비스 계정으로 인증하여 외부 HashiCorp Vault에서 자격 증명에 액세스하도록 데이터 브로커를 설정할 수 있습니다.

"데이터 브로커와 함께 HashiCorp Vault를 사용하는 방법에 대해 자세히 알아보세요." .

S3 버킷에 대한 태그 또는 메타데이터 정의

Amazon S3 버킷에 대한 동기화 관계를 설정할 때 이제 동기화 관계 마법사를 사용하여 대상 S3 버킷의 객체에 저장하려는 태그나 메타데이터를 정의할 수 있습니다.

태그 지정 옵션은 이전에는 동기화 관계 설정의 일부였습니다.

2021년 6월 7일

Google Cloud의 스토리지 클래스

Google Cloud Storage 버킷이 동기화 관계의 대상인 경우 이제 사용할 스토리지 클래스를 선택할 수 있습니다. Cloud Sync 다음과 같은 스토리지 클래스를 지원합니다.

- 기준
- 니어라인
- 콜드라인
- 보관소

2021년 5월 2일

보고서의 오류

이제 보고서에서 발견된 오류를 볼 수 있으며 마지막 보고서나 모든 보고서를 삭제할 수 있습니다.

"구성을 조정하기 위한 보고서 생성 및 보기에 대해 자세히 알아보세요." .

속성 비교

이제 각 동기화 관계에 대해 새로운 비교 기준 설정을 사용할 수 있습니다.

이 고급 설정을 사용하면 Cloud Sync 파일이나 디렉토리가 변경되어 다시 동기화해야 하는지 여부를 결정할 때 특정 속성을 비교해야 하는지 여부를 선택할 수 있습니다.

"동기화 관계 설정 변경에 대해 자세히 알아보세요." .

2021년 4월 11일

독립형 **Cloud Sync** 서비스가 중단되었습니다**.**

독립형 Cloud Sync 서비스는 중단되었습니다. 이제 NetApp 콘솔에서 직접 Cloud Sync 에 액세스할 수 있으며, 모든 동일한 기능을 사용할 수 있습니다.

NetApp 콘솔에 로그인한 후 상단의 동기화 탭으로 전환하여 이전과 마찬가지로 관계를 볼 수 있습니다.

다양한 프로젝트의 **Google Cloud** 버킷

동기화 관계를 설정할 때 데이터 브로커의 서비스 계정에 필요한 권한을 제공하는 경우 다양한 프로젝트의 Google Cloud 버킷에서 선택할 수 있습니다.

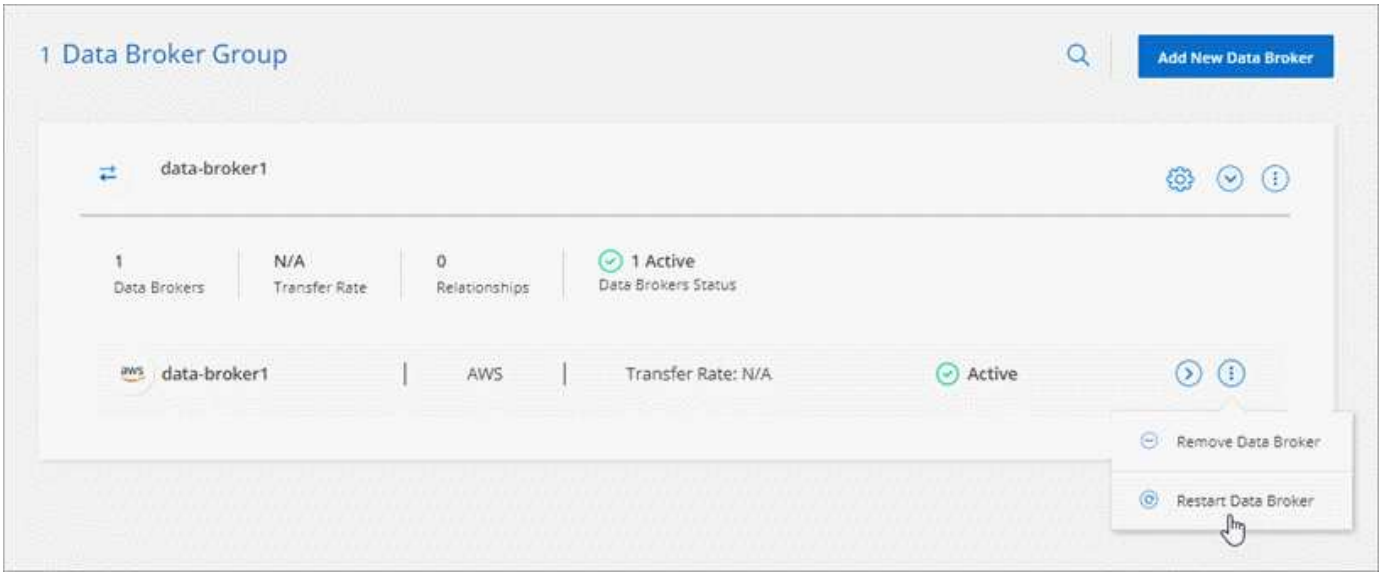
"서비스 계정을 설정하는 방법을 알아보세요" .

Google Cloud Storage와 **S3** 간의 메타데이터

이제 Cloud Sync Google Cloud Storage와 S3 공급업체(AWS S3, StorageGRID, IBM Cloud Object Storage) 간에 메타데이터를 복사합니다.

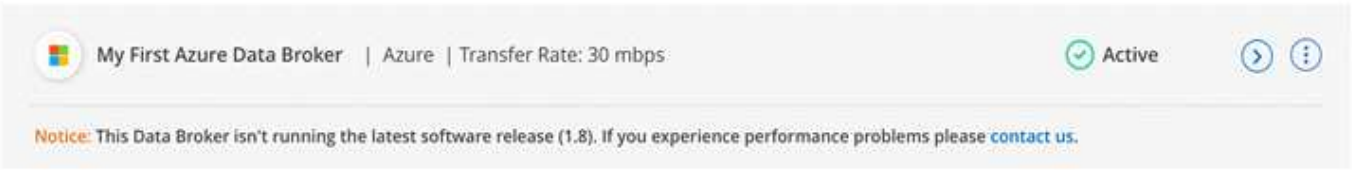
데이터 브로커 재시작

이제 Cloud Sync 에서 데이터 브로커를 다시 시작할 수 있습니다.



최신 릴리스를 실행하지 않을 때의 메시지

이제 Cloud Sync 데이터 브로커가 최신 소프트웨어 릴리스를 실행하지 않는 경우를 식별합니다. 이 메시지는 귀하가 최신 기능을 사용하고 있는지 확인하는 데 도움이 될 수 있습니다.



NetApp 복사 및 동기화의 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼, 장치 또는 기능을 나타냅니다. 이러한 제한 사항을 주의 깊게 검토하세요.

NetApp Copy and Sync는 다음 지역에서는 지원되지 않습니다.

- AWS 정부 지역
- Azure 정부 지역
- 중국

시작하기

NetApp Copy and Sync에 대해 알아보세요

NetApp Copy and Sync는 클라우드나 사내에 있는 모든 대상으로 데이터를 마이그레이션하는 간단하고 안전하며 자동화된 방법을 제공합니다. 파일 기반 NAS 데이터 세트(NFS 또는 SMB), Amazon Simple Storage Service(S3) 객체 형식, NetApp StorageGRID 어플라이언스 또는 기타 클라우드 공급자 객체 저장소 등 어떤 것이든 Copy and Sync가 이를 변환하고 이동할 수 있습니다.

NetApp 콘솔

NetApp Copy and Sync는 NetApp 콘솔을 통해 액세스할 수 있습니다.

NetApp 콘솔은 엔터프라이즈급 온프레미스 및 클라우드 환경 전반에서 NetApp 스토리지 및 데이터 서비스를 중앙에서 관리할 수 있는 기능을 제공합니다. NetApp 데이터 서비스에 액세스하고 사용하려면 콘솔이 필요합니다. 관리 인터페이스로서, 하나의 인터페이스에서 여러 스토리지 리소스를 관리할 수 있습니다. 콘솔 관리자는 기업 내 모든 시스템의 저장소와 서비스에 대한 액세스를 제어할 수 있습니다.

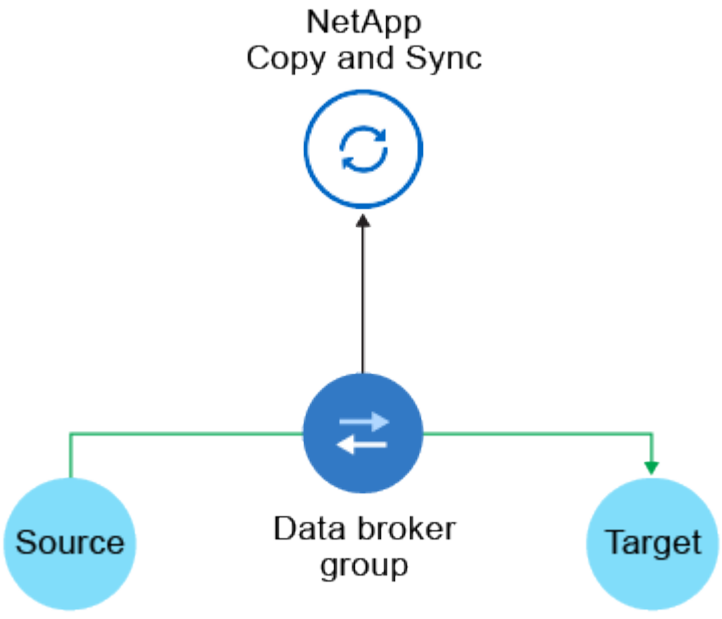
NetApp Console을 사용하려면 라이선스나 구독이 필요하지 않으며, 스토리지 시스템이나 NetApp 데이터 서비스에 대한 연결을 보장하기 위해 클라우드에 Console 에이전트를 배포해야 할 때만 요금이 부과됩니다. 그러나 콘솔에서 액세스할 수 있는 일부 NetApp 데이터 서비스는 라이선스 기반이거나 구독 기반입니다.

자세히 알아보세요 "NetApp 콘솔" .

NetApp 복사 및 동기화 작동 방식

NetApp Copy and Sync는 데이터 브로커 그룹, NetApp 콘솔을 통해 사용 가능한 클라우드 기반 인터페이스, 소스 및 대상으로 구성된 SaaS(Software-as-a-Service) 플랫폼입니다.

다음 이미지는 복사 및 동기화 구성 요소 간의 관계를 보여줍니다.



NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(이를 _동기화 관계_라고 합니다). AWS, Azure, Google Cloud Platform 또는 사내에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 Copy and Sync와 통신하고 몇몇 다른 서비스와 저장소에 접속할 수 있도록 포트 443을 통한 아웃바운드 인터넷 연결이 필요합니다. "엔드포인트 목록 보기" .

최초 복사 후, 복사 및 동기화는 사용자가 설정한 일정에 따라 변경된 데이터를 동기화합니다.

지원되는 저장 유형

복사 및 동기화는 다음과 같은 저장 유형을 지원합니다.

- 모든 NFS 서버
- 모든 SMB 서버
- 아마존 EFS
- ONTAP 용 Amazon FSx
- 아마존 S3
- Azure Blob
- Azure 데이터 레이크 스토리지 Gen2
- Azure NetApp Files
- 상자(미리보기로 제공)
- Cloud Volumes ONTAP
- 구글 클라우드 스토리지
- 구글 드라이브
- IBM 클라우드 객체 스토리지
- 온프레미스 ONTAP 클러스터
- ONTAP S3 스토리지
- SFTP(API만 사용)
- StorageGRID

"지원되는 동기화 관계 보기" .

소송 비용

Copy and Sync를 사용하는 데에는 리소스 요금과 서비스 요금이라는 두 가지 유형의 비용이 있습니다.

자원 요금

리소스 요금은 클라우드에서 하나 이상의 데이터 브로커를 실행하는 데 드는 컴퓨팅 및 저장 비용과 관련됩니다.

서비스 요금

14일 무료 체험 기간이 종료된 후에는 두 가지 방법으로 동기화 관계에 대한 비용을 지불할 수 있습니다. 첫 번째 옵션은 AWS나 Azure에서 구독하는 것입니다. 이를 통해 시간당 또는 연간으로 요금을 지불할 수 있습니다. 두 번째 옵션은 NetApp 에서 직접 라이선스를 구매하는 것입니다.

"라이선싱이 어떻게 작동하는지 알아보세요" .

NetApp Copy and Sync를 위한 빠른 시작

NetApp Copy and Sync를 시작하려면 몇 가지 단계가 필요합니다.


로그인하고 **NetApp** 콘솔을 설정하세요

NetApp 콘솔을 시작했어야 합니다. 여기에는 로그인, 계정 설정, 콘솔 에이전트 배포 및 시스템 생성이 포함됩니다.

다음 중 하나에 대한 동기화 관계를 만들려면 먼저 시스템을 만들거나 검색해야 합니다.

- ONTAP 용 Amazon FSx
- Azure NetApp Files
- Cloud Volumes ONTAP
- 온프레미스 ONTAP 클러스터

Cloud Volumes ONTAP, 온프레미스 ONTAP 클러스터 및 Amazon FSx for ONTAP 에는 콘솔 에이전트가 필요합니다.

- "NetApp 콘솔을 시작하는 방법을 알아보세요"
- "콘솔 에이전트에 대해 자세히 알아보세요"


소스와 타겟을 준비하세요

소스와 타겟이 지원되고 설정되어 있는지 확인하세요. 가장 중요한 요구 사항은 데이터 브로커 그룹과 소스 및 타겟 위치 간의 연결을 확인하는 것입니다.

- "지원되는 관계 보기"
- "소스와 타겟을 준비하세요"


NetApp 데이터 브로커를 위한 위치 준비

NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(이를 _동기화 관계_라고 합니다). AWS, Azure, Google Cloud Platform 또는 사내에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 NetApp Copy and Sync와 통신하고 몇몇 다른 서비스와 저장소에 접속할 수 있도록 포트 443을 통한 아웃바운드 인터넷 연결이 필요합니다. "엔드포인트 목록 보기" .

NetApp Copy and Sync는 동기화 관계를 생성할 때 설치 과정을 안내하며, 이때 클라우드에 데이터 브로커를 배포하거나 자체 Linux 호스트에 대한 설치 스크립트를 다운로드할 수 있습니다.

- "AWS 설치 검토"
- "Azure 설치 검토"
- "Google Cloud 설치 검토"
- "Linux 호스트 설치 검토"

4 첫 번째 동기화 관계를 만드세요

로그인하세요 "NetApp 콘솔" , *동기화*를 선택한 다음 소스와 대상에 대한 선택 항목을 끌어서 놓습니다. 화면의 지시에 따라 설정을 완료하세요. "자세히 알아보기" .

5 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불하세요.

AWS 또는 Azure에 가입하여 사용량에 따라 요금을 지불하거나 연간 요금을 지불하세요. 또는 NetApp 에서 직접 라이선스를 구매하세요. NetApp Copy and Sync의 라이선스 설정 페이지로 가서 설정하기만 하면 됩니다. "자세히 알아보기" .

NetApp Copy and Sync에서 지원되는 동기화 관계

NetApp Copy and Sync를 사용하면 소스에서 대상으로 데이터를 동기화할 수 있습니다. 이것을 동기화 관계라고 합니다. 시작하기 전에 지원되는 관계를 이해해야 합니다.

소스 위치	지원되는 대상 위치
아마존 EFS	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
ONTAP 용 Amazon FSx	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
아마존 S3	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
Azure Blob	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
Azure 데이터 레이크 스토리지 Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • ONTAP 용 FSx • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
Azure NetApp Files	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
상자 [1]	• ONTAP 용 Amazon FSx • 아마존 S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM 클라우드 객체 스토리지 • NFS 서버 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
Cloud Volumes ONTAP	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
구글 클라우드 스토리지	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID
구글 드라이브	• NFS 서버 • SMB 서버

소스 위치	지원되는 대상 위치
IBM 클라우드 객체 스토리지	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
NFS 서버	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • 구글 드라이브 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
온프레미스 ONTAP 클러스터(NFS 또는 SMB)	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
ONTAP S3 스토리지	• 아마존 S3 • Azure 데이터 레이크 스토리지 Gen2 • 구글 클라우드 스토리지 • NFS 서버 • SMB 서버 • StorageGRID • ONTAP S3 스토리지
SFTP [2]	S3

소스 위치	지원되는 대상 위치
SMB 서버	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • 구글 드라이브 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID
StorageGRID	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

참고사항:

1. Box 지원은 미리보기로 제공됩니다.

2. 이 소스/대상과의 동기화 관계는 Copy 및 Sync API를 사용해서만 지원됩니다.
3. Blob 컨테이너가 대상인 경우 특정 Azure Blob 저장소 계층을 선택할 수 있습니다.
    - 뜨거운 보관
    - 시원한 보관
4. Amazon S3가 대상인 경우 특정 S3 스토리지 클래스를 선택할 수 있습니다.
    - 표준(기본 클래스)
    - 지능형 계층화
    - 표준-빈번하지 않은 액세스
    - 1존-접근 빈도 낮음
    - 빙하 심층 기록 보관소
    - Glacier Flexible Retrieval
    - 빙하 즉시 검색
5. Google Cloud Storage 버킷이 대상인 경우 특정 스토리지 클래스를 선택할 수 있습니다.
    - 기준
    - 니어라인
    - 콜드라인
    - 보관소

NetApp Copy and Sync에서 소스와 대상을 준비합니다.

NetApp Copy and Sync에서 소스와 대상이 다음 요구 사항을 충족하는지 확인하세요.

네트워킹

- 소스와 대상은 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

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

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

대상 디렉토리

동기화 관계를 만들면 복사 및 동기화를 통해 기존 대상 디렉토리를 선택한 다음, 선택적으로 해당 디렉토리 내에 새 폴더를 만들 수 있습니다. 따라서 원하는 대상 디렉토리가 이미 존재하는지 확인하세요.

디렉토리 읽기 권한

소스 또는 대상의 모든 디렉토리나 폴더를 표시하려면 복사 및 동기화에 디렉토리나 폴더에 대한 읽기 권한이 필요합니다.

NFS

파일과 디렉토리의 uid/gid를 사용하여 소스/대상에 대한 권한을 정의해야 합니다.

객체 스토리지

- AWS 및 Google Cloud의 경우 데이터 브로커에는 목록 개체 권한이 있어야 합니다(이러한 권한은 데이터 브로커 설치 단계를 따르면 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 브로커는 기본적으로 다음 디렉토리를 무시합니다: .snapshot, ~snapshot, .copy-offload

Amazon S3 버킷 요구 사항

Amazon S3 버킷이 다음 요구 사항을 충족하는지 확인하세요.

Amazon S3에 지원되는 데이터 브로커 위치

S3 스토리지를 포함하는 동기화 관계에는 AWS 또는 사내에 배포된 데이터 브로커가 필요합니다. 어느 경우든, 복사 및 동기화는 설치 중에 데이터 브로커를 AWS 계정과 연결하라는 메시지를 표시합니다.

- "AWS 데이터 브로커를 배포하는 방법을 알아보세요"
- "Linux 호스트에 데이터 브로커를 설치하는 방법을 알아보세요"

지원되는 **AWS** 지역

중국 지역을 제외한 모든 지역이 지원됩니다.

다른 **AWS** 계정의 **S3** 버킷에 필요한 권한

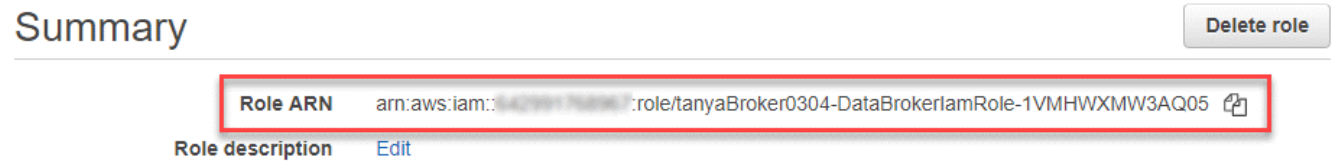
동기화 관계를 설정할 때 데이터 브로커와 연결되지 않은 AWS 계정에 있는 S3 버킷을 지정할 수 있습니다.

"이 JSON 파일에 포함된 권한"데이터 브로커가 액세스할 수 있도록 해당 S3 버킷에 적용해야 합니다. 이러한 권한을 통해 데이터 브로커는 버킷에서 데이터를 복사하거나 버킷에 있는 객체를 나열할 수 있습니다.

JSON 파일에 포함된 권한에 대해 다음 사항을 참고하세요.

1. _<BucketName>_은 데이터 브로커와 연결되지 않은 AWS 계정에 있는 버킷의 이름입니다.
2. _<RoleARN>_은 다음 중 하나로 대체되어야 합니다.
    - Linux 호스트에 데이터 브로커를 수동으로 설치한 경우 _RoleARN_은 데이터 브로커를 배포할 때 AWS 자격 증명을 제공한 AWS 사용자의 ARN이어야 합니다.
    - CloudFormation 템플릿을 사용하여 AWS에 데이터 브로커가 배포된 경우 _RoleARN_은 템플릿에서 생성된 IAM 역할의 ARN이어야 합니다.

      EC2 콘솔로 이동하여 데이터 브로커 인스턴스를 선택한 다음 설명 탭에서 IAM 역할을 선택하면 역할 ARN을 찾을 수 있습니다. 그러면 IAM 콘솔에서 역할 ARN이 포함된 요약 페이지가 표시됩니다.



Azure Blob 저장소 요구 사항

Azure Blob 저장소가 다음 요구 사항을 충족하는지 확인하세요.

Azure Blob에 지원되는 데이터 브로커 위치

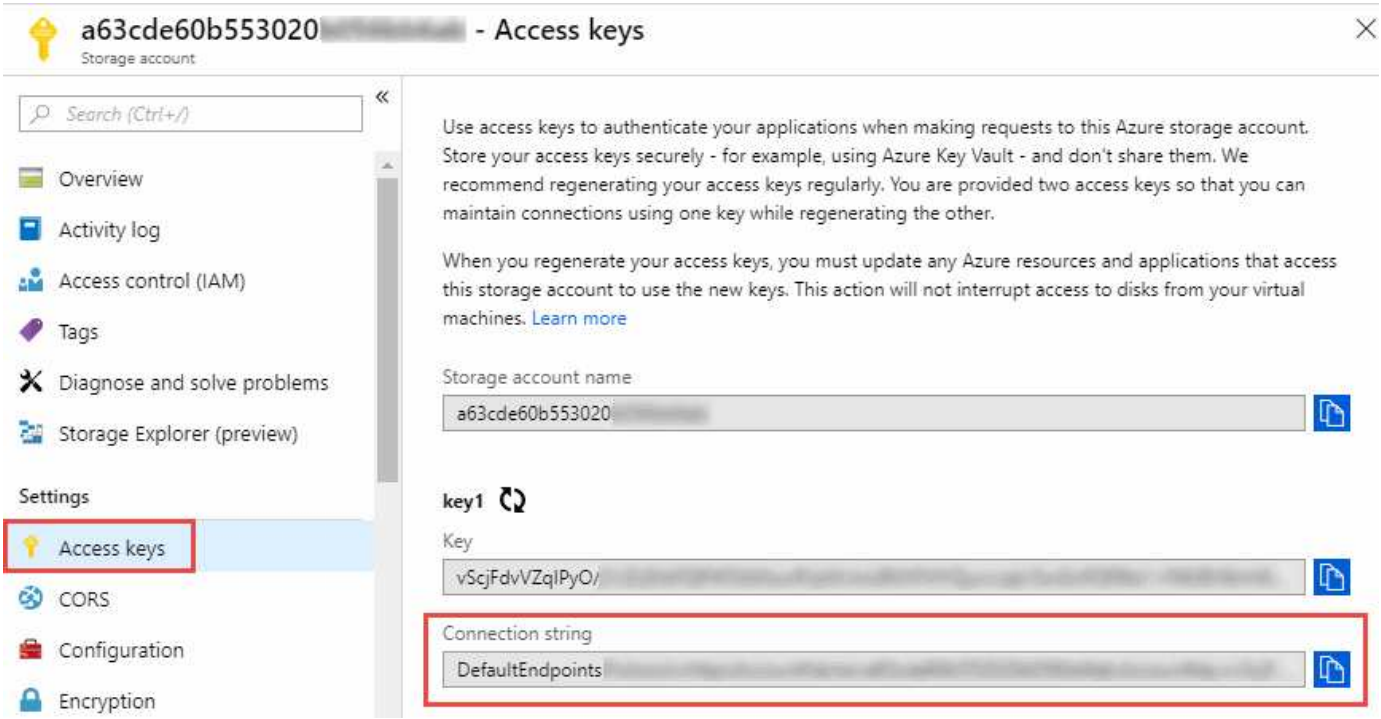
동기화 관계에 Azure Blob 저장소가 포함된 경우 데이터 브로커는 어느 위치에나 상주할 수 있습니다.

지원되는 Azure 지역

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

Azure Blob 및 NFS/SMB를 포함하는 관계에 대한 연결 문자열

Azure Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화 관계를 만들 때는 저장소 계정 연결 문자열을 사용하여 Copy 및 Sync를 제공해야 합니다.

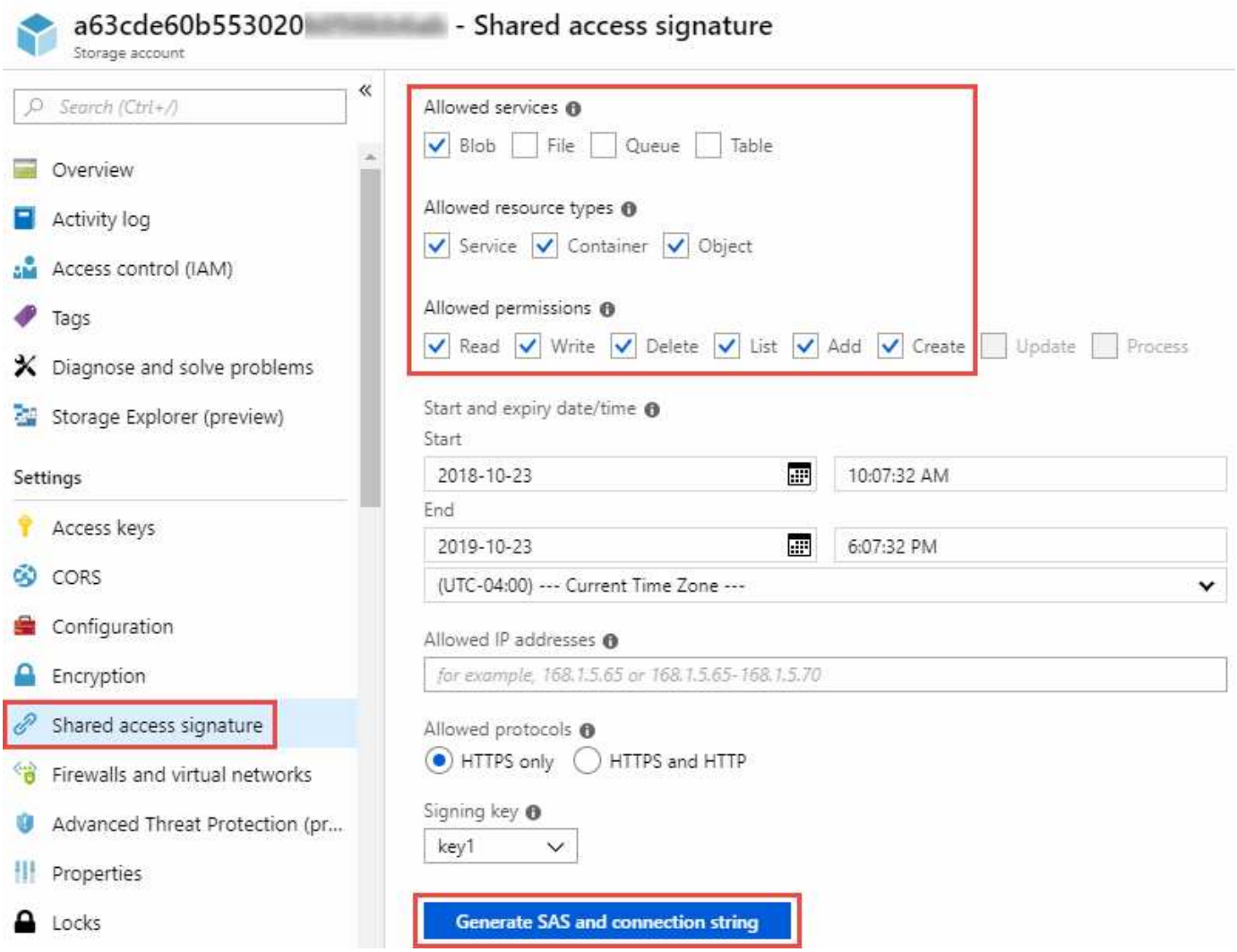


두 Azure Blob 컨테이너 간에 데이터를 동기화하려면 연결 문자열에 다음을 포함해야 합니다. "공유 액세스 서명" (SAS). Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화할 때 SAS를 사용하는 옵션도 있습니다.

SAS는 Blob 서비스와 모든 리소스 유형(서비스, 컨테이너, 개체)에 대한 액세스를 허용해야 합니다. SAS에는 다음 권한도 포함되어야 합니다.

- 소스 Blob 컨테이너의 경우: 읽기 및 나열

- 대상 Blob 컨테이너의 경우: 읽기, 쓰기, 나열, 추가 및 생성



Azure Blob 컨테이너를 포함하는 Continuous Sync 관계를 구현하도록 선택하는 경우 일반 연결 문자열이나 SAS 연결 문자열을 사용할 수 있습니다. SAS 연결 문자열을 사용하는 경우 가까운 미래에 만료되도록 설정해서는 안 됩니다.

Azure 데이터 레이크 스토리지 Gen2

Azure Data Lake를 포함하는 동기화 관계를 만들 때는 저장소 계정 연결 문자열을 사용하여 Copy and Sync를 제공해야 합니다. SAS(공유 액세스 서명)가 아닌 일반 연결 문자열이어야 합니다.

Azure NetApp Files 요구 사항

Azure NetApp Files 에서 데이터를 동기화할 때는 Premium 또는 Ultra 서비스 수준을 사용합니다. 디스크 서비스 수준이 표준인 경우 오류 및 성능 문제가 발생할 수 있습니다.

적절한 서비스 수준을 결정하는 데 도움이 필요하면 솔루션 아키텍트에게 문의하세요. 볼륨 크기와 볼륨 계층은 얻을 수 있는 처리량을 결정합니다.

"Azure NetApp Files 서비스 수준 및 처리량에 대해 자세히 알아보세요." .

상자 요구 사항

- Box를 포함하는 동기화 관계를 만들려면 다음 자격 증명을 제공해야 합니다.
  - 클라이언트 ID
  - 클라이언트 비밀번호
  - 개인 키
  - 공개 키 ID
  - 암호문구
  - 엔터프라이즈 ID
- Amazon S3에서 Box로 동기화 관계를 생성하는 경우 다음 설정이 1로 설정된 통합 구성을 갖는 데이터 브로커 그룹을 사용해야 합니다.
  - 스캐너 동시성
  - 스캐너 프로세스 제한
  - 전송자 동시성
  - 전송자 프로세스 제한

  "데이터 브로커 그룹에 대한 통합 구성을 정의하는 방법을 알아보세요." .

Google Cloud Storage 버킷 요구 사항

Google Cloud Storage 버킷이 다음 요구 사항을 충족하는지 확인하세요.

Google Cloud Storage에 지원되는 데이터 브로커 위치

Google Cloud Storage를 포함하는 동기화 관계에는 Google Cloud 또는 사내에 배포된 데이터 브로커가 필요합니다. 복사 및 동기화는 동기화 관계를 생성할 때 데이터 브로커 설치 프로세스를 안내합니다.

- "Google Cloud 데이터 브로커를 배포하는 방법을 알아보세요"
- "Linux 호스트에 데이터 브로커를 설치하는 방법을 알아보세요"

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 버킷에서 선택할 수 있습니다. "서비스 계정을 설정하는 방법을 알아보세요" .

SnapMirror 대상에 대한 권한

동기화 관계의 소스가 SnapMirror 대상(읽기 전용)인 경우 "읽기/나열" 권한만으로도 소스에서 대상으로 데이터를 동기화할 수 있습니다.

Google Cloud 버킷 암호화

고객 관리 KMS 키 또는 기본 Google 관리 키를 사용하여 대상 Google Cloud 버킷을 암호화할 수 있습니다. 버킷에 이미 KMS 암호화가 추가된 경우 기본 Google 관리 암호화가 재정의됩니다.

고객 관리 KMS 키를 추가하려면 데이터 브로커를 사용해야 합니다. "올바른 권한" , 키는 버킷과 같은 지역에 있어야 합니다.

구글 드라이브

Google Drive를 포함하는 동기화 관계를 설정하는 경우 다음을 제공해야 합니다.

- 데이터를 동기화하려는 Google Drive 위치에 액세스할 수 있는 사용자의 이메일 주소
- Google Drive에 액세스할 수 있는 권한이 있는 Google Cloud 서비스 계정의 이메일 주소
- 서비스 계정의 개인 키

서비스 계정을 설정하려면 Google 문서의 지침을 따르세요.

- "서비스 계정 및 자격 증명을 만듭니다."
- "도메인 전체 권한을 서비스 계정에 위임합니다."

OAuth 범위 필드를 편집할 때 다음 범위를 입력하세요.

- \ https://www.googleapis.com/auth/drive
- \ https://www.googleapis.com/auth/drive.file

NFS 서버 요구 사항

- NFS 서버는 NetApp 시스템이거나 NetApp 아닌 시스템일 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, 4.2가 지원됩니다.

  원하는 버전을 서버에서 활성화해야 합니다.

- ONTAP 시스템에서 NFS 데이터를 동기화하려면 SVM에 대한 NFS 내보내기 목록에 대한 액세스가 활성화되어 있는지 확인하세요(vserver nfs modify -vserver *svm_name* -showmount enabled).

  ⓘ ONTAP 9.2부터 showmount의 기본 설정은 _enabled_입니다.

ONTAP 요구 사항

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

ONTAP S3 스토리지 요구 사항

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

- ONTAP S3에 연결된 LIF의 IP 주소
- ONTAP 이 사용하도록 구성된 액세스 키와 비밀 키

SMB 서버 요구 사항

- SMB 서버는 NetApp 시스템이거나 NetApp 아닌 시스템일 수 있습니다.
- SMB 서버에 대한 권한이 있는 자격 증명을 복사 및 동기화에 제공해야 합니다.
  - 소스 SMB 서버의 경우 다음 권한이 필요합니다: 나열 및 읽기.

    백업 운영자 그룹의 구성원은 소스 SMB 서버를 통해 지원을 받습니다.

  - 대상 SMB 서버에는 다음 권한이 필요합니다: 나열, 읽기, 쓰기.
- 파일 서버는 데이터 브로커 호스트가 필요한 포트를 통해 내보내기에 액세스할 수 있도록 허용해야 합니다.
  - 139 TCP
  - 445 TCP
  - 137-138 UDP
- SMB 버전 1.0, 2.0, 2.1, 3.0 및 3.11이 지원됩니다.
- "관리자" 그룹에 소스 및 대상 폴더에 대한 "전체 제어" 권한을 부여합니다.

  이 권한을 부여하지 않으면 데이터 브로커가 파일이나 디렉토리에 대한 ACL을 가져올 수 있는 충분한 권한이 없을 수 있습니다. 이런 경우 다음 오류가 발생합니다. "getxattr error 95"

숨겨진 디렉토리 및 파일에 대한 SMB 제한

SMB 제한은 SMB 서버 간에 데이터를 동기화할 때 숨겨진 디렉터리와 파일에 영향을 미칩니다. 원본 SMB 서버에 있는 디렉토리나 파일 중 하나가 Windows를 통해 숨겨진 경우, 숨김 속성은 대상 SMB 서버로 복사되지 않습니다.

대소문자 구분 제한으로 인한 SMB 동기화 동작

SMB 프로토콜은 대소문자를 구분하지 않으므로 대문자와 소문자가 동일하게 처리됩니다. 동기화 관계에 SMB 서버가 포함되어 있고 데이터가 이미 대상에 있는 경우, 이러한 동작으로 인해 파일 덮어쓰기 및 디렉터리 복사 오류가 발생할 수 있습니다.

예를 들어, 소스에 "a"라는 파일이 있고, 대상에 "A"라는 파일이 있다고 가정해 보겠습니다. 복사 및 동기화를 통해 "a"라는 파일을 대상에 복사하면, 파일 "A"는 소스의 파일 "a"로 덮어쓰여집니다.

디렉토리의 경우 소스에 "b"라는 디렉토리가 있고, 타겟에 "B"라는 디렉토리가 있다고 가정해 보겠습니다. Copy and Sync가 "b"라는 디렉토리를 대상에 복사하려고 하면, Copy and Sync는 해당 디렉토리가 이미 존재한다는 오류를 수신합니다. 결과적으로 Copy and Sync는 항상 "b"라는 디렉토리를 복사하는 데 실패합니다.

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

NetApp Copy and Sync에 대한 네트워킹 개요

NetApp Copy and Sync를 위한 네트워킹에는 데이터 브로커 그룹과 소스 및 대상 위치 간의 연결, 그리고 포트 443을 통한 데이터 브로커의 아웃바운드 인터넷 연결이 포함됩니다.

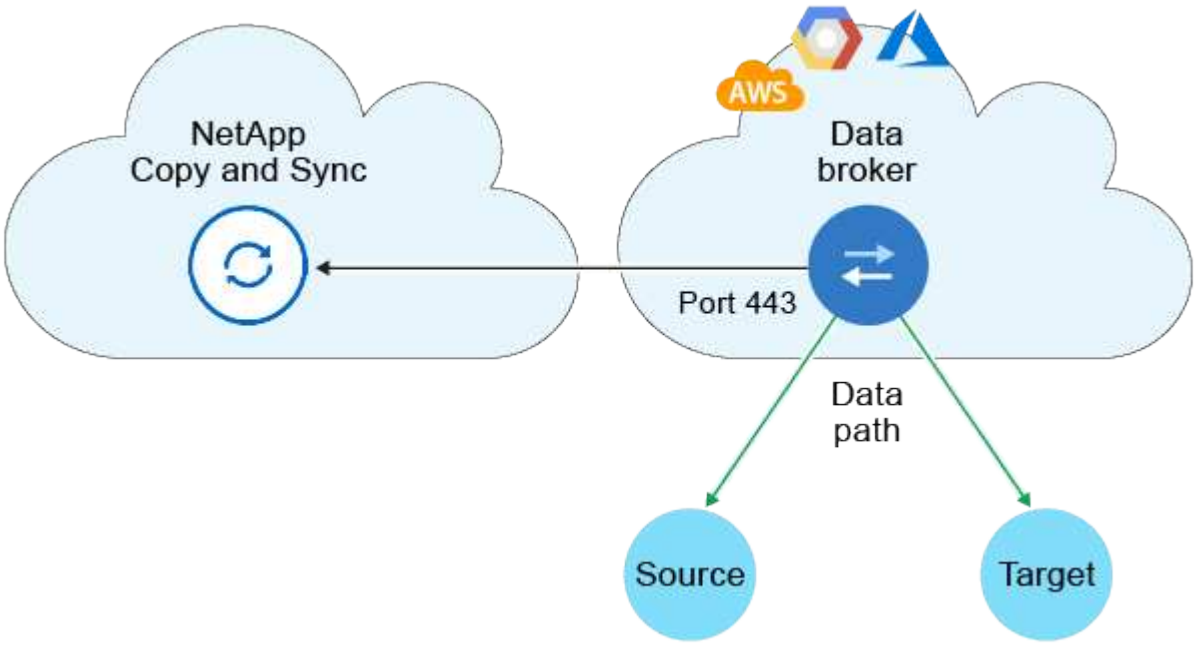
데이터 브로커 위치

데이터 브로커 그룹은 클라우드나 회사 내부에 설치된 하나 이상의 데이터 브로커로 구성됩니다.

클라우드의 데이터 브로커

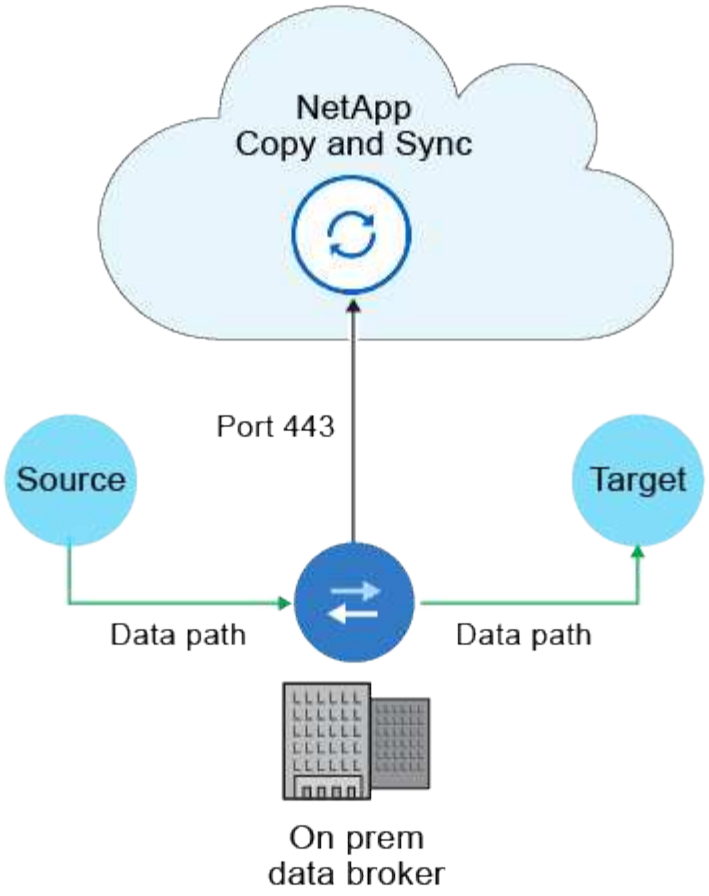
다음 이미지는 AWS, Google Cloud 또는 Azure의 클라우드에서 실행되는 데이터 브로커를 보여줍니다. 데이터 브로커에 연결되어 있는 한 소스와 타겟은 어느 위치에나 있을 수 있습니다. 예를 들어, 데이터 센터에서 클라우드 제공업체로 VPN 연결이 있을 수 있습니다.

Copy and Sync가 AWS, Azure 또는 Google Cloud에 데이터 브로커를 배포하는 경우, 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.



귀사 구내의 데이터 브로커

다음 이미지는 데이터 센터에서 온프레미스로 실행되는 데이터 브로커를 보여줍니다. 다시 말해, 소스와 타겟은 데이터 브로커에 연결되어 있는 한 어느 위치에나 있을 수 있습니다.



네트워킹 요구 사항

- 소스와 대상은 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

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

- 데이터 브로커는 포트 443을 통해 복사 및 동기화 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.
- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

네트워킹 엔드포인트

NetApp 데이터 브로커는 Copy and Sync와 통신하고 몇몇 다른 서비스와 저장소에 접속하기 위해 포트 443을 통한 아웃바운드 인터넷 액세스가 필요합니다. 특정 작업을 수행하려면 로컬 웹 브라우저에서도 엔드포인트에 액세스해야 합니다. 아웃바운드 연결을 제한해야 하는 경우 아웃바운드 트래픽에 대한 방화벽을 구성할 때 다음 엔드포인트 목록을 참조하세요.

데이터 브로커 엔드포인트

데이터 브로커는 다음 엔드포인트에 접속합니다.

엔드포인트	목적
\ https://olcentgbl.trafficmanager.net	데이터 브로커 호스트에 대한 CentOS 패키지를 업데이트하기 위해 저장소에 문의합니다. 이 엔드포인트는 CentOS 호스트에 데이터 브로커를 수동으로 설치하는 경우에만 접속됩니다.
\ https://rpm.nodesource.com \ https://registry.npmjs.org \ https://nodejs.org:	개발에 사용되는 Node.js, npm 및 기타 타사 패키지를 업데이트하기 위해 저장소에 문의합니다.
\ https://tgz.pm2.io	복사 및 동기화를 모니터링하는 데 사용되는 타사 패키지인 PM2를 업데이트하기 위한 저장소에 액세스합니다.
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	Copy and Sync가 작업(파일 대기, 작업 등록, 데이터 브로커에 업데이트 전달)에 사용하는 AWS 서비스에 문의합니다.
\ 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 참조하세요."^]	동기화 관계에 S3 버킷이 포함된 경우 Amazon S3에 연락합니다.
\ https://s3.amazonaws.com/	Copy and Sync에서 데이터 브로커 로그를 다운로드하면 데이터 브로커가 로그 디렉토리를 압축하고 해당 로그를 us-east-1 지역의 미리 정의된 S3 버킷에 업로드합니다.
\ https://storage.googleapis.com/	동기화 관계에서 GCP 버킷을 사용하는 경우 Google Cloud에 문의합니다.
https://storage-account.blob.core.windows.netAzure Data Lake Gen2를 사용하는 경우:https://storage-account.dfs.core.windows.net[] 여기서 _storage-account_는 사용자의 소스 저장소 계정입니다.	사용자의 Azure 스토리지 계정 주소에 대한 프록시를 엽니다.
\ https://cf.cloudsync.netapp.com \ https://repo.cloudsync.netapp.com	Copy and Sync에 문의하세요.
\ https://support.netapp.com	동기화 관계에 BYOL 라이선스를 사용하는 경우 NetApp 지원팀에 문의하세요.
\ https://fedoraproject.org	설치 및 업데이트 중에 데이터 브로커 가상 머신에 7z를 설치합니다. NetApp 기술 지원팀에 AutoSupport 메시지를 보내려면 7z가 필요합니다.
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	데이터 브로커가 AWS에 배포되거나 사내에 배포되고 AWS 자격 증명이 제공되는 경우 AWS 자격 증명을 확인합니다. 데이터 브로커는 배포 중, 업데이트 시, 재시작 시 이 엔드포인트에 접속합니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com	새로운 동기화 관계에 대한 소스 파일을 선택하기 위해 분류를 사용하는 경우 NetApp 데이터 분류에 문의하세요.
\ https://pubsub.googleapis.com	Google 스토리지 계정에서 지속적인 동기화 관계를 만드는 경우.

엔드포인트	목적
https://storage-account.queue.core.windows.net\ https://management.azure.com/subscriptions/ ${subscriptionId} /resourceGroups/${resourceGroup}/providers/Microsoft.EventGrid/* 여기서 _storage-account_는 사용자의 원본 저장소 계정이고, _subscriptionid_는 원본 구독 ID이고, _resourceGroup_은 원본 리소스 그룹입니다.	Azure Storage 계정에서 지속적인 동기화 관계를 만드는 경우.

웹 브라우저 엔드포인트

문제 해결을 위해 로그를 다운로드하려면 웹 브라우저가 다음 엔드포인트에 액세스해야 합니다.

logs.cloudsync.netapp.com:443

NetApp Copy and Sync에 로그인하세요

NetApp 콘솔을 사용하여 NetApp Copy and Sync에 로그인합니다.

콘솔에 로그인하려면 NetApp 지원 사이트 자격 증명을 사용하거나 이메일과 비밀번호를 사용하여 NetApp 클라우드 로그인에 가입할 수 있습니다. "로그인에 대해 자세히 알아보세요" .

NetApp Copy and Sync는 ID 액세스 관리를 사용하여 각 사용자가 특정 작업에 대해 갖는 액세스 권한을 관리합니다.

필수 **NetApp** 콘솔 역할 조직 관리자 역할. "NetApp 콘솔 액세스 역할에 대해 알아보세요" .

단계

1. 웹 브라우저를 열고 이동하세요 "NetApp 콘솔" .

   NetApp 콘솔 로그인 페이지가 나타납니다.

2. 콘솔에 로그인합니다.
3. 콘솔 왼쪽 탐색에서 모바일 > *복사 및 동기화*를 선택합니다.

데이터 브로커 설치

NetApp Copy and Sync를 위해 **AWS**에서 새로운 데이터 브로커 만들기

NetApp Copy and Sync에 대한 새로운 데이터 브로커 그룹을 생성할 때 VPC의 새 EC2 인스턴스에 데이터 브로커 소프트웨어를 배포하려면 Amazon Web Services를 선택하세요.

NetApp Copy and Sync는 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

클라우드나 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치하는 옵션도 있습니다. "자세히 알아보기" .

지원되는 **AWS** 지역

중국 지역을 제외한 모든 지역이 지원됩니다.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 복사 및 동기화 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Copy and Sync가 AWS에 데이터 브로커를 배포하면 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다. 설치 과정에서 프록시 서버를 사용하도록 데이터 브로커를 구성할 수 있습니다.

  아웃바운드 연결을 제한해야 하는 경우 다음을 참조하세요."데이터 브로커가 연락하는 엔드포인트 목록" .

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

AWS에 데이터 브로커를 배포하는 데 필요한 권한

데이터 브로커를 배포하는 데 사용하는 AWS 사용자 계정에는 다음에 포함된 권한이 있어야 합니다. "이 NetApp 제공 정책" .

AWS 데이터 브로커에서 자체 **IAM** 역할을 사용하기 위한 요구 사항

Copy and Sync가 데이터 브로커를 배포하면 데이터 브로커 인스턴스에 대한 IAM 역할이 생성됩니다. 원하는 경우 사용자 고유의 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.

- EC2 서비스는 신뢰할 수 있는 엔터티로서 IAM 역할을 맡을 수 있어야 합니다.
- "이 JSON 파일에 정의된 권한"데이터 브로커가 제대로 작동하려면 IAM 역할에 연결되어야 합니다.

데이터 브로커를 배포할 때 IAM 역할을 지정하려면 아래 단계를 따르세요.

데이터 브로커 생성

새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 생성할 때 AWS에 데이터 브로커를 설치하는 방법을 설명합니다.

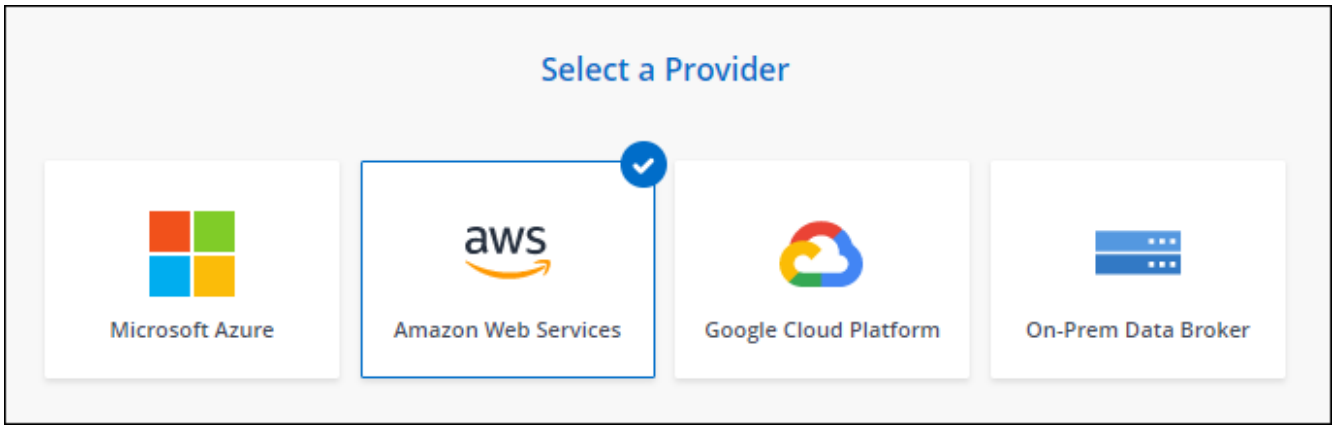
단계

1. "복사 및 동기화에 로그인하세요" .

2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *Amazon Web Services*를 선택합니다.



5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.
6. AWS 액세스 키를 입력하면 Copy and Sync가 사용자를 대신하여 AWS에서 데이터 브로커를 생성할 수 있습니다.

   키는 저장되지 않으며 다른 목적으로 사용되지 않습니다.

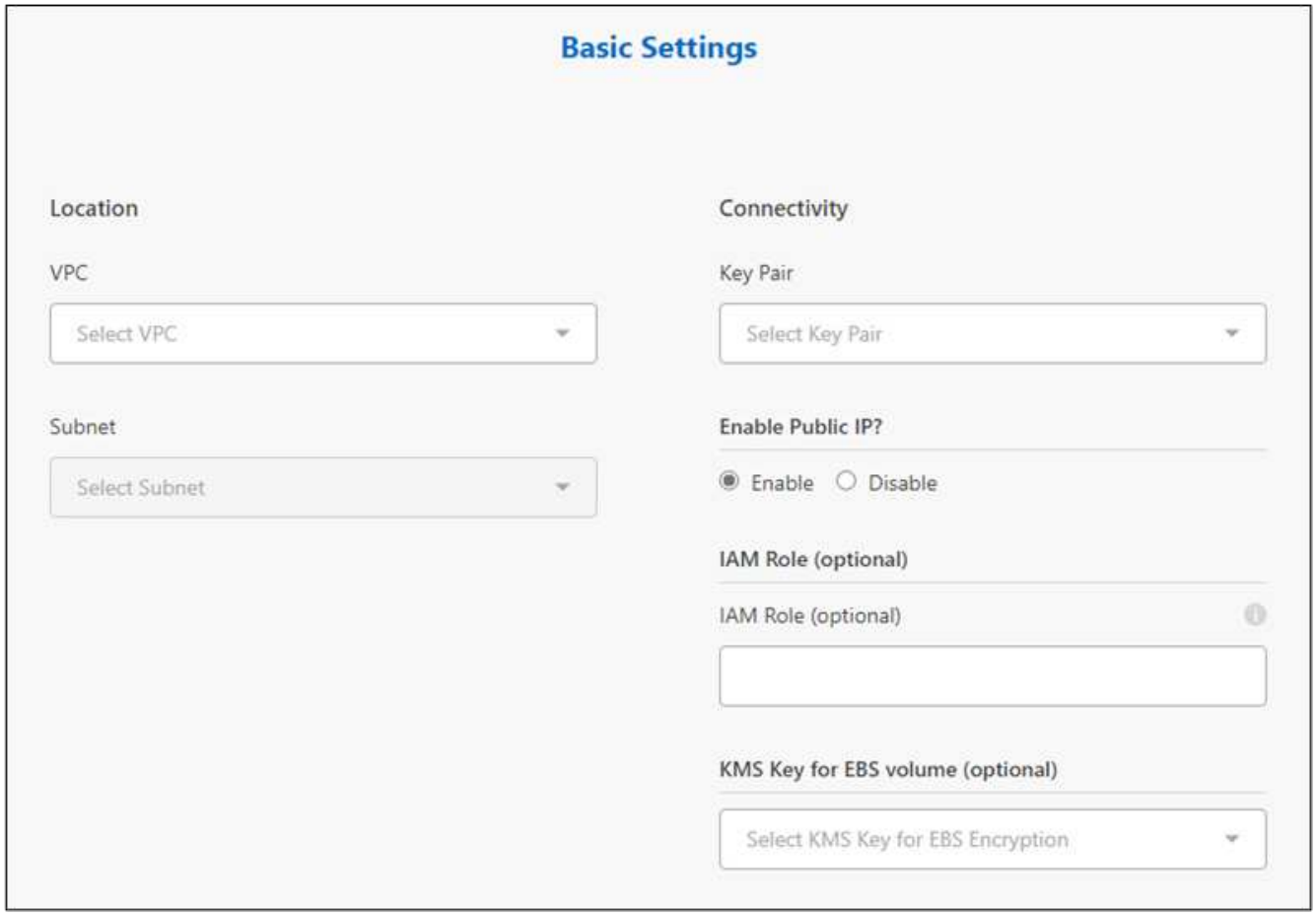
   액세스 키를 제공하지 않으려면 페이지 하단의 링크를 선택하여 대신 CloudFormation 템플릿을 사용하세요. 이 옵션을 사용하면 AWS에 직접 로그인하므로 자격 증명을 제공할 필요가 없습니다.

   다음 비디오는 CloudFormation 템플릿을 사용하여 데이터 브로커 인스턴스를 시작하는 방법을 보여줍니다.

   AWS CloudFormation 템플릿에서 데이터 브로커 시작

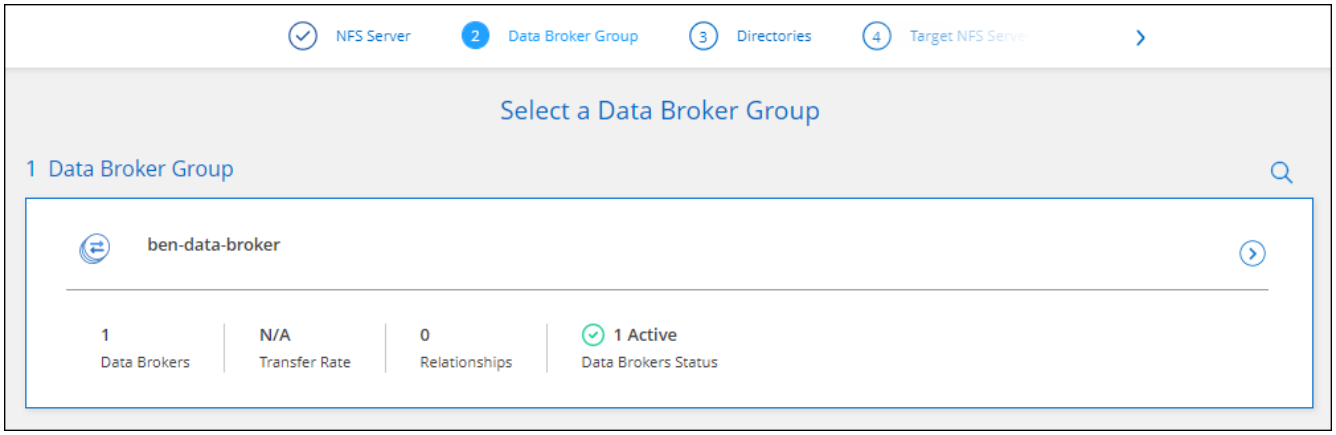
7. AWS 액세스 키를 입력한 경우 인스턴스의 위치를 선택하고, 키 쌍을 선택하고, 공용 IP 주소를 활성화할지 여부를 선택하고, 기존 IAM 역할을 선택하거나, 필드를 비워 두면 복사 및 동기화가 해당 역할을 자동으로 생성합니다. KMS 키를 사용하여 데이터 브로커를 암호화하는 옵션도 있습니다.

   자신의 IAM 역할을 선택하는 경우필요한 권한을 제공해야 합니다. .



8. VPC에서 인터넷 접속에 프록시가 필요한 경우 프록시 구성을 지정합니다.
9. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.

   다음 이미지는 AWS에 성공적으로 배포된 인스턴스를 보여줍니다.



10. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.

결과

AWS에 데이터 브로커를 배포하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브로커 그룹을 추가 동기화 관계와 함께 사용할 수 있습니다.

데이터 브로커 인스턴스에 대한 세부 정보

Copy and Sync는 다음 구성을 사용하여 AWS에서 데이터 브로커를 생성합니다.

Node.js 호환성
v21.2.0

인스턴스 유형
해당 지역에서 사용 가능한 경우 m5n.xlarge, 그렇지 않은 경우 m5.xlarge

vCPU
4

숫양
16GB

운영 체제
아마존 리눅스 2023

디스크 크기 및 유형
10GB GP2 SSD

NetApp Copy and Sync를 위해 Azure에서 새 데이터 브로커 만들기

NetApp Copy and Sync에 대한 새 데이터 브로커 그룹을 만들 때 VNet의 새 가상 머신에 데이터 브로커 소프트웨어를 배포하려면 Microsoft Azure를 선택하세요. NetApp Copy and Sync는 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

클라우드나 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치하는 옵션도 있습니다. "자세히 알아보기" .

지원되는 **Azure** 지역

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

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Copy and Sync 서비스에 대한 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Copy and Sync가 Azure에 데이터 브로커를 배포하면 필요한 아웃바운드 통신을 활성화하는 보안 그룹을 만듭니다.

  아웃바운드 연결을 제한해야 하는 경우 다음을 참조하세요."데이터 브로커가 연락하는 엔드포인트 목록" .

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

Azure에서 데이터 브로커를 배포하는 데 필요한 권한

데이터 브로커를 배포하는 데 사용하는 Azure 사용자 계정에 다음 권한이 있는지 확인하세요.

```
{
    "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",
                    "Microsoft.Storage/storageAccounts/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/write",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/delete",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action",
                    "Microsoft.EventGrid/systemTopics/read",
                    "Microsoft.EventGrid/systemTopics/write",
                    "Microsoft.EventGrid/systemTopics/delete",
                    "Microsoft.EventGrid/eventSubscriptions/write",
                    "Microsoft.Storage/storageAccounts/write"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write"

"Microsoft.Network/networkSecurityGroups/securityRules/read",
                    "Microsoft.Network/networkSecurityGroups/read",
```

```
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}
```

메모:

1. 다음 권한은 다음을 활성화하려는 경우에만 필요합니다. "연속 동기화 설정" Azure에서 다른 클라우드 저장소 위치로의 동기화 관계에 대해:
    - 'Microsoft.Storage/storageAccounts/read',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',

- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/삭제',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action',
- 'Microsoft.EventGrid/systemTopics/read',
- 'Microsoft.EventGrid/systemTopics/write',
- 'Microsoft.EventGrid/systemTopics/삭제',
- 'Microsoft.EventGrid/eventSubscriptions/write',
- 'Microsoft.Storage/storageAccounts/write'

또한 Azure에서 Continuous Sync를 구현하려는 경우 할당 가능한 범위를 리소스 그룹 범위가 아닌 구독 범위로 설정해야 합니다.

2. 다음 권한은 데이터 브로커 생성에 대한 보안을 직접 선택하려는 경우에만 필요합니다.
   - "Microsoft.Network/networkSecurityGroups/securityRules/read"
   - "Microsoft.Network/networkSecurityGroups/read"

인증 방법

데이터 브로커를 배포할 때 가상 머신에 대한 인증 방법(암호 또는 SSH 공개-개인 키 쌍)을 선택해야 합니다.

키 쌍 생성에 대한 도움말은 다음을 참조하세요. "Azure 설명서: Azure에서 Linux VM에 대한 SSH 공개-개인 키 쌍 만들기 및 사용" .

데이터 브로커 생성

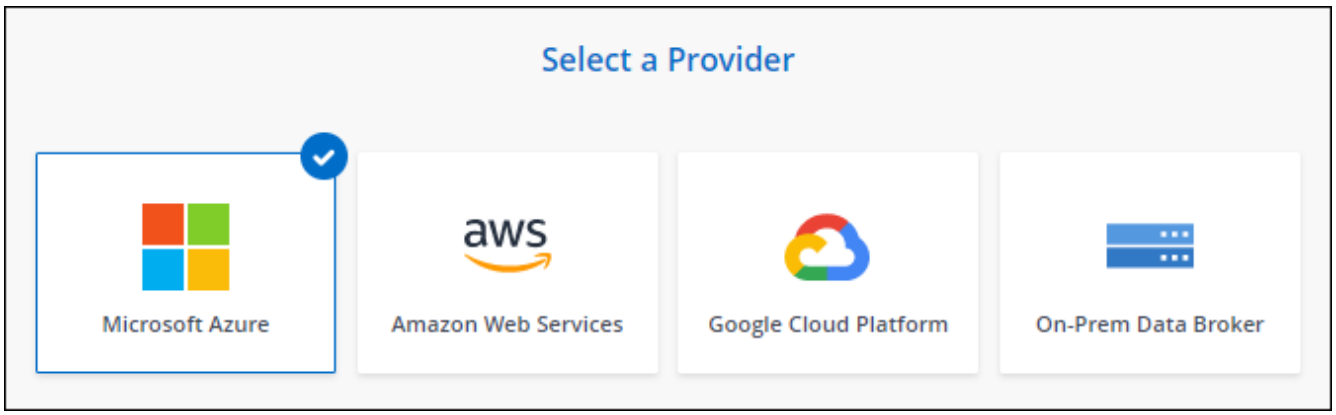
새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 만들 때 Azure에 데이터 브로커를 설치하는 방법을 설명합니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

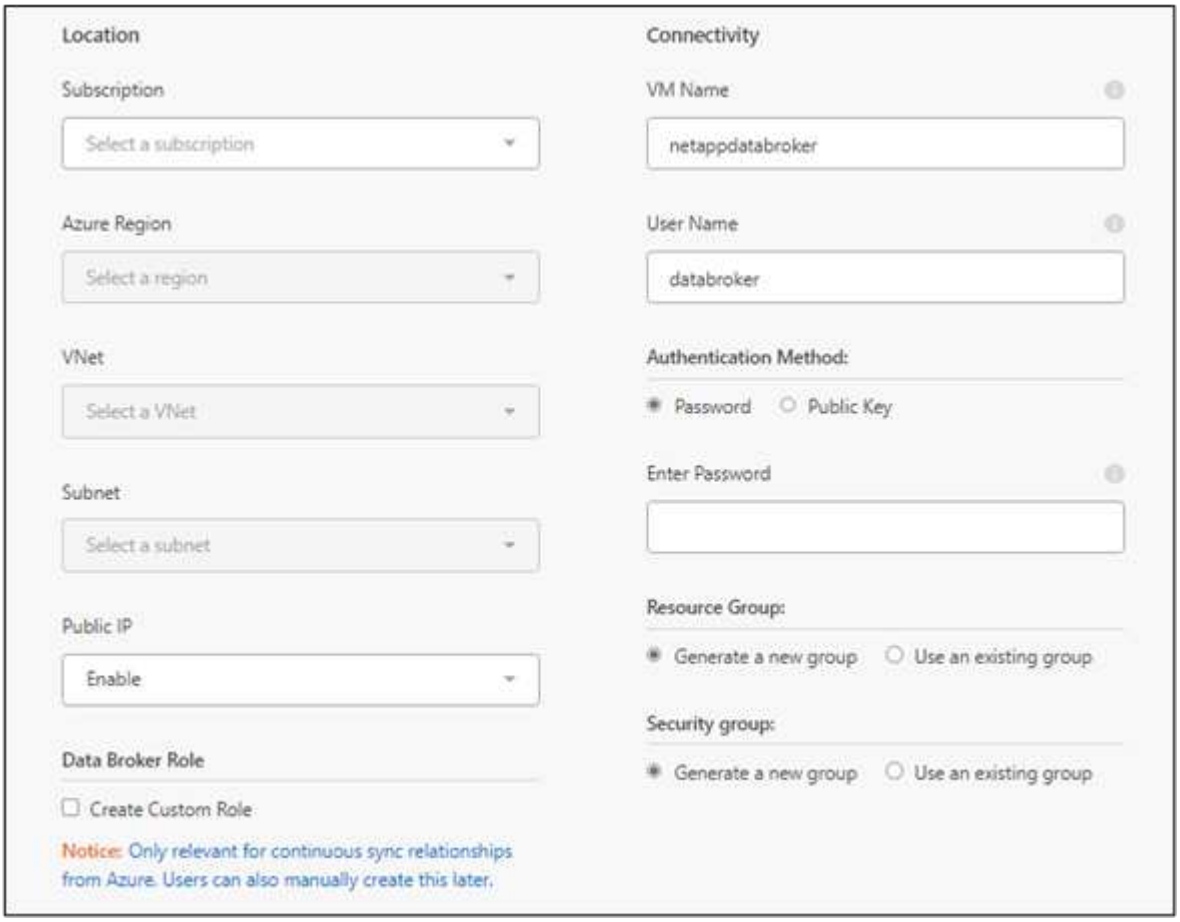
4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *Microsoft Azure*를 선택합니다.



5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.
6. 메시지가 표시되면 Microsoft 계정에 로그인하세요. 메시지가 표시되지 않으면 *Azure에 로그인*을 선택하세요.

   이 양식은 Microsoft에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

7. 데이터 브로커의 위치를 선택하고 가상 머신에 대한 기본 세부 정보를 입력합니다.



지속적인 동기화 관계를 구현하려면 데이터 브로커에 사용자 지정 역할을 할당해야 합니다. 이 작업은 브로커가 생성된 후 수동으로 수행할 수도 있습니다.

8. VNet에서 인터넷 접속에 프록시가 필요한 경우 프록시 구성을 지정합니다.
9. *계속*을 선택하세요. 데이터 브로커에 S3 권한을 추가하려면 AWS 액세스 키와 비밀 키를 입력하세요.

10. *계속*을 선택하고 배포가 완료될 때까지 페이지를 열어 두세요.

    이 과정은 최대 7분이 걸릴 수 있습니다.

11. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.
12. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.

결과

Azure에 데이터 브로커를 배포하고 새로운 동기화 관계를 만들었습니다. 이 데이터 브로커를 추가 동기화 관계와 함께 사용할 수 있습니다.

관리자 동의가 필요하다는 메시지를 받으셨나요?

Microsoft에서 Copy and Sync가 사용자를 대신하여 조직의 리소스에 액세스하려면 권한이 필요하므로 관리자 승인이 필요하다고 알리는 경우 두 가지 옵션이 있습니다.

1. AD 관리자에게 다음 권한을 부여해 달라고 요청하세요.

   Azure에서 *관리 센터 > Azure AD > 사용자 및 그룹 > 사용자 설정*으로 이동하여 *사용자는 앱이 자신을 대신하여 회사 데이터에 액세스하는 데 동의할 수 있음*을 활성화합니다.

2. 다음 URL을 사용하여 AD 관리자에게 *CloudSync-AzureDataBrokerCreator*에 대한 동의를 요청하세요(이것이 관리자 동의 엔드포인트입니다).

   \ https://login.microsoftonline.com/ {여기에 테넌트 ID를 입력하세요}/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 대로, 앱 URL은 https://cloudsync.netapp.com 이고 애플리케이션 클라이언트 ID는 8ee4ca3a-bafa-4831-97cc-5a38923cab85입니다.

데이터 브로커 **VM**에 대한 세부 정보

복사 및 동기화는 다음 구성을 사용하여 Azure에 데이터 브로커를 만듭니다.

Node.js 호환성
: v21.2.0

VM 유형
: 표준 DS4 v2

vCPU
: 8

숫양
: 28GB

운영 체제

로키 리눅스 9.0

디스크 크기 및 유형

64GB 프리미엄 SSD

Google Cloud에서 NetApp Copy and Sync를 위한 새로운 데이터 브로커 만들기

NetApp Copy and Sync에 대한 새로운 데이터 브로커 그룹을 생성할 때 Google Cloud Platform을 선택하여 Google Cloud VPC의 새로운 가상 머신 인스턴스에 데이터 브로커 소프트웨어를 배포합니다. NetApp Copy and Sync는 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

클라우드나 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치하는 옵션도 있습니다. "자세히 알아보기" .

지원되는 Google Cloud 지역

모든 지역이 지원됩니다.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 복사 및 동기화 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Copy and Sync가 Google Cloud에 데이터 브로커를 배포하면 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.

  아웃바운드 연결을 제한해야 하는 경우 다음을 참조하세요."데이터 브로커가 연락하는 엔드포인트 목록" .

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

Google Cloud에 데이터 브로커를 배포하는 데 필요한 권한

데이터 브로커를 배포하는 Google Cloud 사용자에게 다음 권한이 있는지 확인하세요.

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

서비스 계정에 필요한 권한

데이터 브로커를 배포할 때 다음 권한이 있는 서비스 계정을 선택해야 합니다.

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update
- iam.serviceAccounts.signJwt
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

참고사항:

1. "iam.serviceAccounts.signJwt" 권한은 외부 HashiCorp 볼트를 사용하도록 데이터 브로커를 설정하려는 경우에만 필요합니다.
2. "pubsub.*" 및 "storage.buckets.update" 권한은 Google Cloud Storage에서 다른 클라우드 스토리지 위치로의 동기화 관계에 대해 지속적인 동기화 설정을 활성화하려는 경우에만 필요합니다. "연속 동기화 옵션에 대해 자세히 알아보세요" .
3. "cloudkms.cryptoKeys.list" 및 "cloudkms.keyRings.list" 권한은 대상 Google Cloud Storage 버킷에서 고객 관리 KMS 키를 사용하려는 경우에만 필요합니다.

데이터 브로커 생성

새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 생성할 때 Google Cloud에 데이터 브로커를 설치하는 방법을 설명합니다.

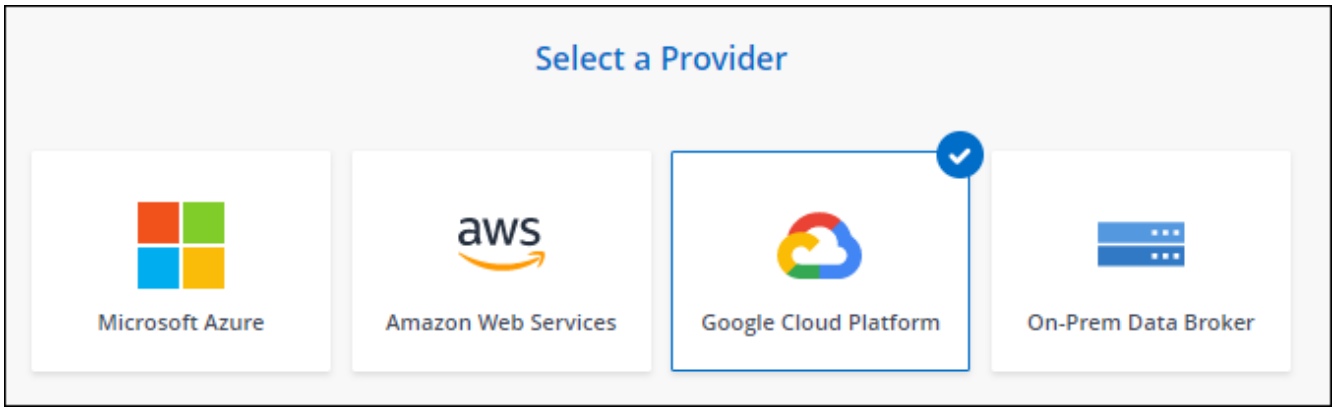
단계

1. "복사 및 동기화에 로그인하세요" .

2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *Google Cloud Platform*을 선택합니다.

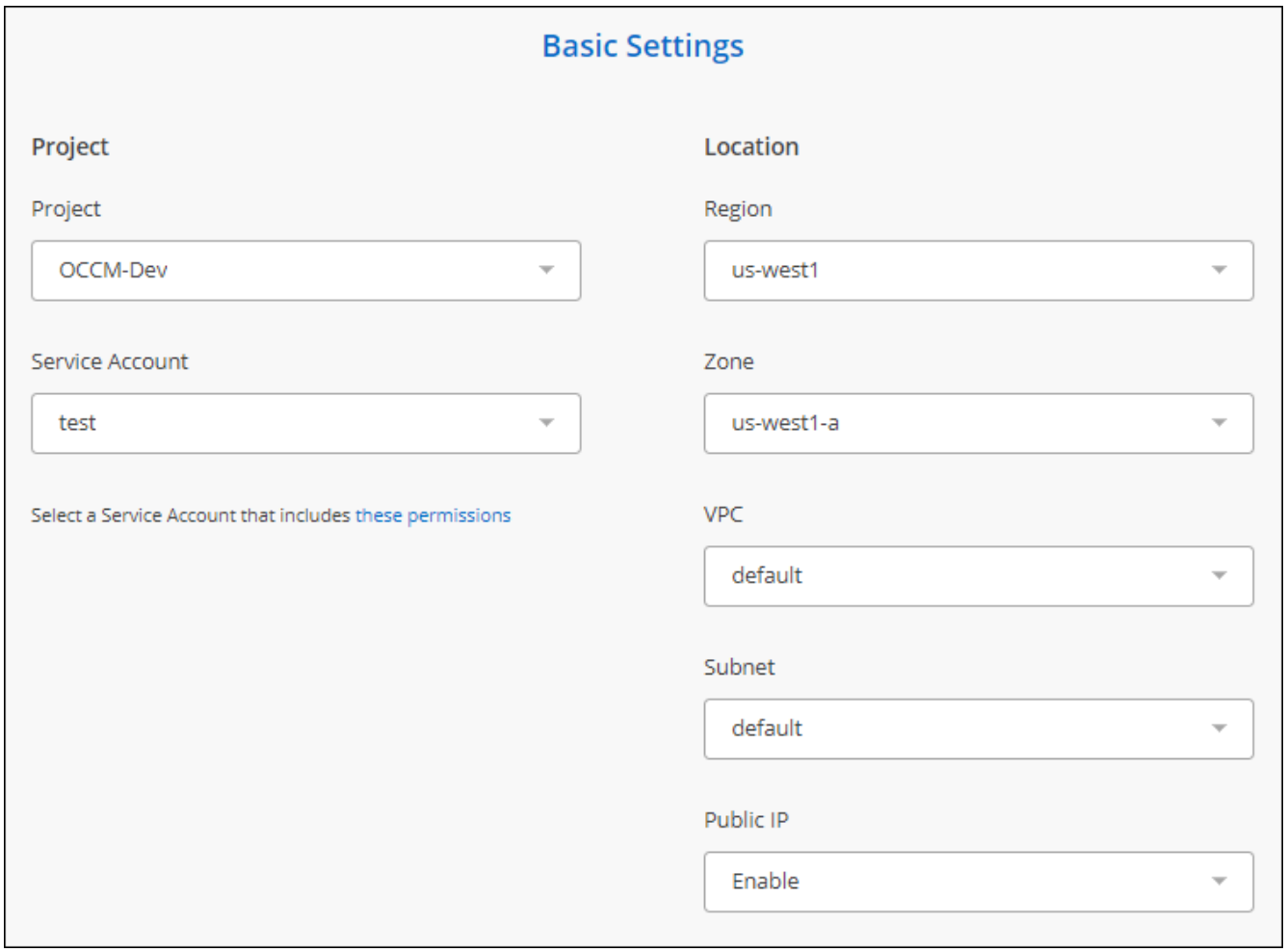


5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.
6. 메시지가 표시되면 Google 계정으로 로그인하세요.

   이 양식은 Google에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

7. 프로젝트와 서비스 계정을 선택한 다음, 데이터 브로커의 위치를 선택합니다. 여기에는 공용 IP 주소를 활성화할지 비활성화할지 여부도 포함됩니다.

   공용 IP 주소를 활성화하지 않으면 다음 단계에서 프록시 서버를 정의해야 합니다.



8. VPC에서 인터넷 접속에 프록시가 필요한 경우 프록시 구성을 지정합니다.

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

9. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.

   인스턴스를 배포하는 데 약 5~10분이 걸립니다. 인스턴스를 사용할 수 있게 되면 자동으로 새로 고쳐지는 복사 및 동기화에서 진행 상황을 모니터링할 수 있습니다.

10. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.

결과

Google Cloud에 데이터 브로커를 배포하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브로커를 추가 동기화 관계와 함께 사용할 수 있습니다.

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

동기화 관계를 생성하고 Google Cloud Storage를 소스 또는 대상으로 선택하면 복사 및 동기화를 통해 데이터 브로커의 서비스 계정에서 사용할 수 있는 버킷을 선택할 수 있습니다. 기본적으로 여기에는 데이터 브로커 서비스 계정과 동일한 프로젝트에 있는 버킷이 포함됩니다. 하지만 필요한 권한을 제공하면 다른 프로젝트에서 버킷을 선택할 수 있습니다.

단계

1. Google Cloud Platform 콘솔을 열고 Cloud Storage 서비스를 로드합니다.
2. 동기화 관계에서 소스 또는 대상으로 사용할 버킷의 이름을 선택합니다.
3. *권한*을 선택하세요.
4. *추가*를 선택하세요.
5. 데이터 브로커 서비스 계정의 이름을 입력하세요.
6. 제공하는 역할을 선택하세요위에 표시된 것과 동일한 권한 .
7. *저장*을 선택하세요.

결과

동기화 관계를 설정하면 이제 동기화 관계에서 해당 버킷을 소스 또는 대상으로 선택할 수 있습니다.

데이터 브로커 **VM** 인스턴스에 대한 세부 정보

복사 및 동기화는 다음 구성을 사용하여 Google Cloud에 데이터 브로커를 생성합니다.

Node.js 호환성
: v21.2.0

기계 유형
: n2-표준-4

vCPU
: 4

숫양
: 15GB

운영 체제
: 로키 리눅스 9.0

디스크 크기 및 유형
: 20GB HDD pd-standard

NetApp Copy and Sync를 위해 Linux 호스트에 데이터 브로커 설치

NetApp Copy and Sync에 대한 새로운 데이터 브로커 그룹을 생성할 때 온프레미스 데이터 브로커 옵션을 선택하여 온프레미스 Linux 호스트 또는 클라우드의 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치합니다. NetApp Copy and Sync는 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

Linux 호스트 요구 사항

- **Node.js** 호환성: v21.2.0
- 운영체제:
  - CentOS 8.0 및 8.5

CentOS Stream은 지원되지 않습니다.

- Red Hat Enterprise Linux 8.5, 8.8, 8.9 및 9.4
- 로키 리눅스 9
- Ubuntu Server 20.04 LTS, 23.04 LTS 및 24.04 LTS
- 수세 리눅스 엔터프라이즈 서버 15 SP1

명령 `yum update` 데이터 브로커를 설치하기 전에 호스트에서 실행해야 합니다.

Red Hat Enterprise Linux 시스템은 Red Hat Subscription Management에 등록해야 합니다. 등록되지 않은 경우, 시스템은 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 접근할 수 없습니다.

- 램: 16GB
- **CPU**: 4코어
- 사용 가능한 디스크 공간: 10GB
- **SELinux**: 호스트에서 SELinux를 비활성화하는 것이 좋습니다.

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

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- Linux 호스트는 소스와 대상에 연결되어 있어야 합니다.
- 파일 서버는 Linux 호스트가 내보내기에 액세스할 수 있도록 허용해야 합니다.
- AWS로의 아웃바운드 트래픽을 위해서는 Linux 호스트에서 포트 443이 열려 있어야 합니다(데이터 브로커는 Amazon SQS 서비스와 지속적으로 통신합니다).
- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

AWS에 대한 액세스 활성화

S3 버킷을 포함하는 동기화 관계로 데이터 브로커를 사용하려는 경우 AWS 액세스를 위해 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 프로그래밍 방식 액세스와 특정 권한이 있는 AWS 사용자에 대한 AWS 키를 제공해야 합니다.

단계

1. 다음을 사용하여 IAM 정책을 만듭니다. "이 NetApp 제공 정책"

   "AWS 지침 보기"

2. 프로그래밍 방식 액세스 권한이 있는 IAM 사용자를 만듭니다.

"AWS 지침 보기"

데이터 브로커 소프트웨어를 설치할 때 AWS 키를 지정해야 하므로 반드시 복사하세요.

Google Cloud에 대한 액세스 활성화

Google Cloud Storage 버킷을 포함하는 동기화 관계로 데이터 브로커를 사용하려는 경우 Google Cloud 액세스를 위해 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 특정 권한이 있는 서비스 계정에 대한 키를 제공해야 합니다.

단계

1. 아직 스토리지 관리자 권한이 있는 Google Cloud 서비스 계정이 없다면 하나 만드세요.
2. JSON 형식으로 저장된 서비스 계정 키를 만듭니다.

   "Google Cloud 지침 보기"

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

   키를 생성하면 파일이 생성되어 컴퓨터에 다운로드됩니다.

3. JSON 파일을 Linux 호스트에 저장합니다.

Microsoft Azure에 대한 액세스 활성화

Azure에 대한 액세스는 동기화 관계 마법사에서 저장소 계정과 연결 문자열을 제공하여 관계별로 정의됩니다.

데이터 브로커 설치

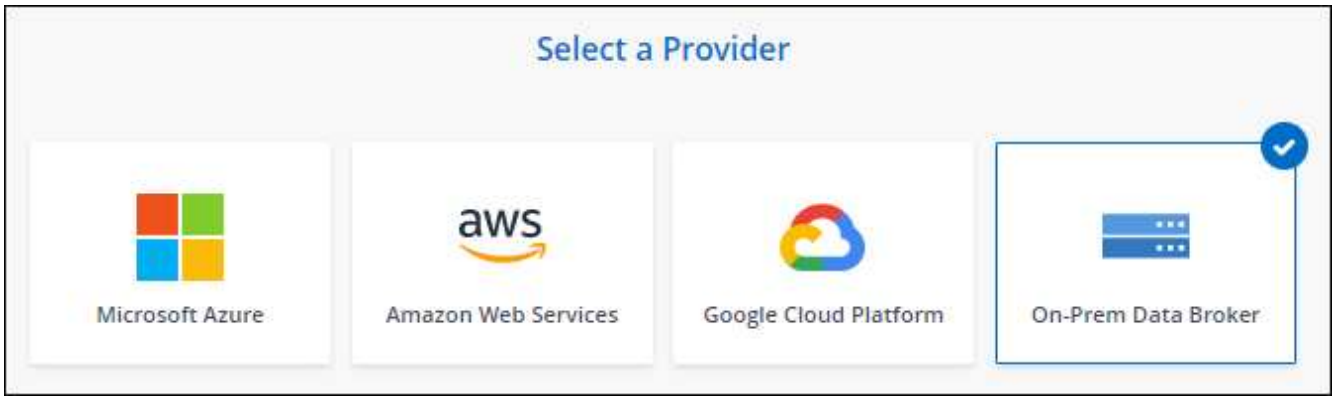
동기화 관계를 만들 때 Linux 호스트에 데이터 브로커를 설치할 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *온프레미스 데이터 브로커*를 선택합니다.



해당 옵션은 *온프레미스 데이터 브로커*로 표시되어 있지만, 이는 사내 또는 클라우드의 Linux 호스트에 적용됩니다.

5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.

   곧 지침 페이지가 로드됩니다. 다음 지침을 따라야 합니다. 이 지침에는 설치 프로그램을 다운로드할 수 있는 고유 링크가 포함되어 있습니다.

6. 지침 페이지에서:

   a. **AWS**, **Google Cloud** 또는 둘 다에 대한 액세스를 활성화할지 선택합니다.

   b. 설치 옵션을 선택하세요: 프록시 없음, 프록시 서버 사용, 인증과 함께 프록시 서버 사용.

      사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.

   c. 명령을 사용하여 데이터 브로커를 다운로드하고 설치합니다.

      다음 단계에서는 가능한 각 설치 옵션에 대한 자세한 내용을 제공합니다. 설치 옵션에 따라 정확한 명령을 얻으려면 지침 페이지를 따르세요.

   d. 설치 프로그램을 다운로드하세요:

      - 프록시 없음:

        ```
        curl <URI> -o data_broker_installer.sh
        ```

      - 프록시 서버 사용:

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

      - 인증과 함께 프록시 서버를 사용합니다.

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

        URI

        복사 및 동기화는 설치 파일의 URI를 지침 페이지에 표시합니다. 이 URI는 온프레미스 데이터 브로커를 배포하기 위한 프롬프트를 따르면 로드됩니다. 해당 URI는 여기서 반복되지 않습니다. 링크는 동적으로 생성되고 한 번만 사용할 수 있기 때문입니다. Copy and Sync에서 URI를 얻으려면 다음 단계를 따르세요. .

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

> 아래 나열된 각 명령에는 AWS 액세스 및 Google Cloud 액세스에 대한 매개변수가 포함되어 있습니다. 설치 옵션에 따라 정확한 명령을 얻으려면 지침 페이지를 따르세요.

- 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>
```

- 인증을 통한 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> -u
<proxy_username> -w <proxy_password>
```

AWS 키

이는 사용자가 준비해야 하는 키입니다.다음 단계를 따르세요 . AWS 키는 온프레미스 또는 클라우드 네트워크에서 실행되는 데이터 브로커에 저장됩니다. NetApp 데이터 브로커 외부의 키를 사용하지 않습니다.

JSON 파일

이것은 당신이 준비해야 할 서비스 계정 키가 포함된 JSON 파일입니다.다음 단계를 따르세요 .

7. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.
8. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.

NetApp 복사 및 동기화 사용

소스와 대상 간 데이터 동기화

NetApp Copy and Sync에서 개체 스토리지 간 데이터를 동기화하기 위한 데이터 브로커 준비

NetApp Copy and Sync에서 개체 스토리지 간에 데이터를 동기화하려는 경우(예: Amazon S3에서 Azure Blob으로) 동기화 관계를 생성하기 전에 데이터 브로커 그룹을 준비해야 합니다.

이 작업에 관하여

데이터 브로커 그룹을 준비하려면 스캐너 구성을 수정해야 합니다. 구성을 수정하지 않으면 이 동기화 관계에서 성능 문제가 발생할 수 있습니다.

시작하기 전에

개체 스토리지 간에 데이터를 동기화하는 데 사용하는 데이터 브로커 그룹은 이러한 유형의 동기화 관계만 관리해야 합니다. 데이터 브로커 그룹이 다른 유형의 동기화 관계(예: NFS 대 NFS 또는 개체 스토리지 대 SMB)를 관리하는 경우 해당 동기화 관계의 성능이 부정적인 영향을 받을 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. 복사 및 동기화에서 *데이터 브로커 관리*를 선택합니다.
3. 선택하다 
4. 스캐너 구성을 업데이트하세요.
   a. *스캐너 동시성*을 *1*로 변경합니다.
   b. *스캐너 프로세스 제한*을 *1*로 변경합니다.
5. *구성 통합*을 선택합니다.

결과

복사 및 동기화는 데이터 브로커 그룹의 구성을 업데이트합니다.

다음은 무엇인가요?

방금 구성한 데이터 브로커 그룹을 사용하여 개체 스토리지 간의 동기화 관계를 만들 수 있습니다.

NetApp Copy and Sync에서 동기화 관계 만들기

동기화 관계를 생성하면 NetApp Copy and Sync가 소스에서 대상으로 파일을 복사합니다. 최초 복사 후, 복사 및 동기화는 24시간마다 변경된 데이터를 동기화합니다.

일부 유형의 동기화 관계를 만들려면 먼저 NetApp 콘솔에서 시스템을 만들어야 합니다.

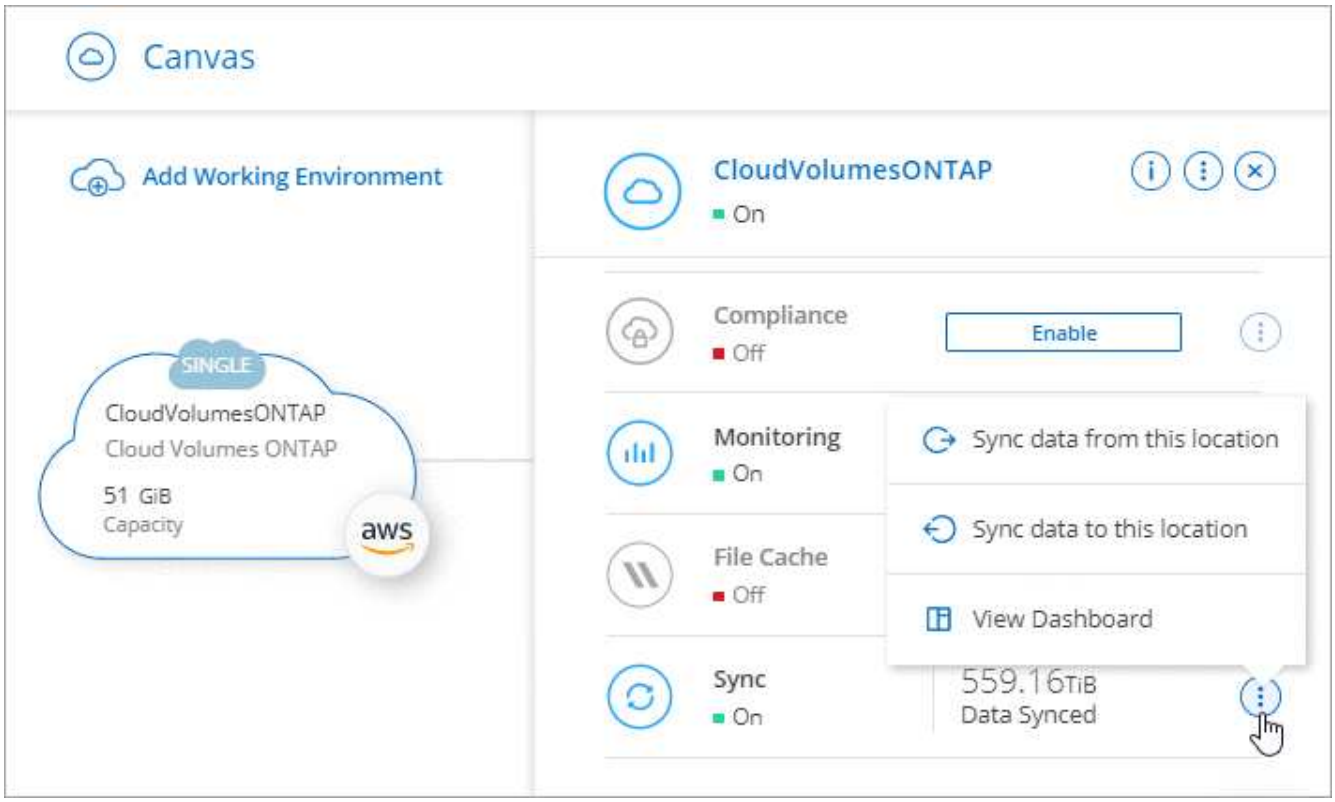
특정 유형의 시스템에 대한 동기화 관계 생성

다음 중 하나에 대한 동기화 관계를 만들려면 먼저 시스템을 만들거나 검색해야 합니다.

- ONTAP 용 Amazon FSx
- Azure NetApp Files
- Cloud Volumes ONTAP
- 온프레미스 ONTAP 클러스터

단계

1. "복사 및 동기화에 로그인하세요" .
2. 시스템을 생성하거나 발견합니다.
   - "Amazon FSx for ONTAP 시스템 생성"
   - "Azure NetApp Files 설정 및 검색"
   - "AWS에서 Cloud Volumes ONTAP 출시"
   - "Azure에서 Cloud Volumes ONTAP 시작"
   - "Google Cloud에서 Cloud Volumes ONTAP 출시"
   - "기존 Cloud Volumes ONTAP 시스템 추가"
   - "ONTAP 클러스터 검색"
3. *시스템 페이지*를 선택하세요.
4. 위에 나열된 유형 중 하나와 일치하는 시스템을 선택하세요.
5. 동기화 옆에 있는 작업 메뉴를 선택하세요.



6. 이 위치에서 데이터 동기화 또는 *이 위치에 데이터 동기화*를 선택하고 화면의 지시에 따라 동기화 관계를 설정합니다.

다른 유형의 동기화 관계 만들기

다음 단계를 사용하여 Amazon FSx for ONTAP, Azure NetApp Files, Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터가 아닌 지원되는 스토리지 유형과 데이터를 동기화합니다. 아래 단계에서는 NFS 서버에서 S3 버킷으로 동기화 관계를 설정하는 방법을 보여주는 예를 제공합니다.

1. NetApp 콘솔에서 *동기화*를 선택합니다.
2. 동기화 관계 정의 페이지에서 소스와 대상을 선택합니다.

   다음 단계에서는 NFS 서버에서 S3 버킷으로 동기화 관계를 만드는 방법의 예를 보여줍니다.

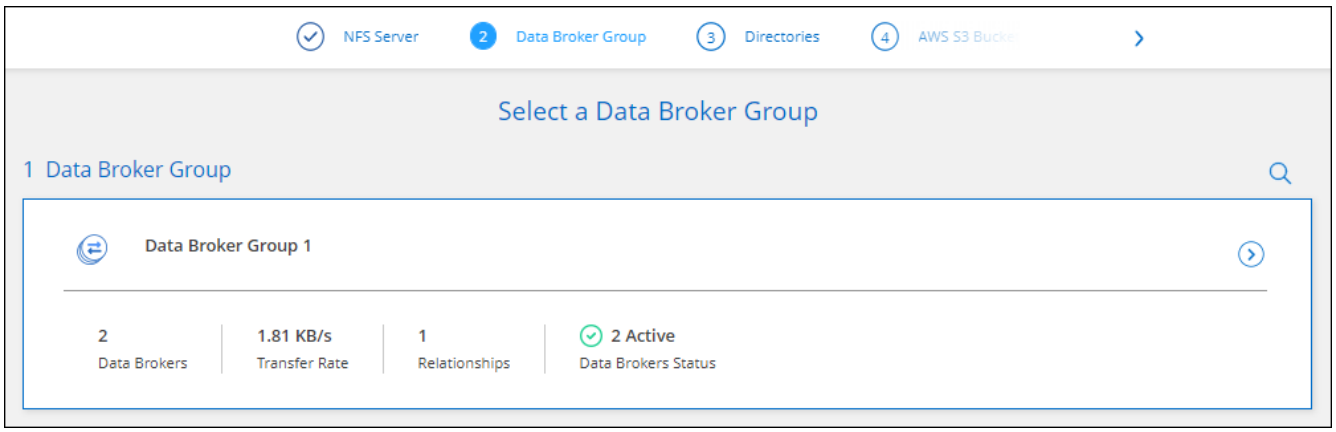
3. **NFS** 서버 페이지에서 AWS와 동기화하려는 NFS 서버의 IP 주소나 정규화된 도메인 이름을 입력합니다.
4. 데이터 브로커 그룹 페이지에서 프롬프트에 따라 AWS, Azure 또는 Google Cloud Platform에서 데이터 브로커 가상 머신을 만들거나 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치합니다.

   자세한 내용은 다음 페이지를 참조하세요.

   - "AWS에서 데이터 브로커 만들기"
   - "Azure에서 데이터 브로커 만들기"
   - "Google Cloud에서 데이터 브로커 만들기"

- "Linux 호스트에 데이터 브로커 설치"

5. 데이터 브로커를 설치한 후 *계속*을 선택하세요.



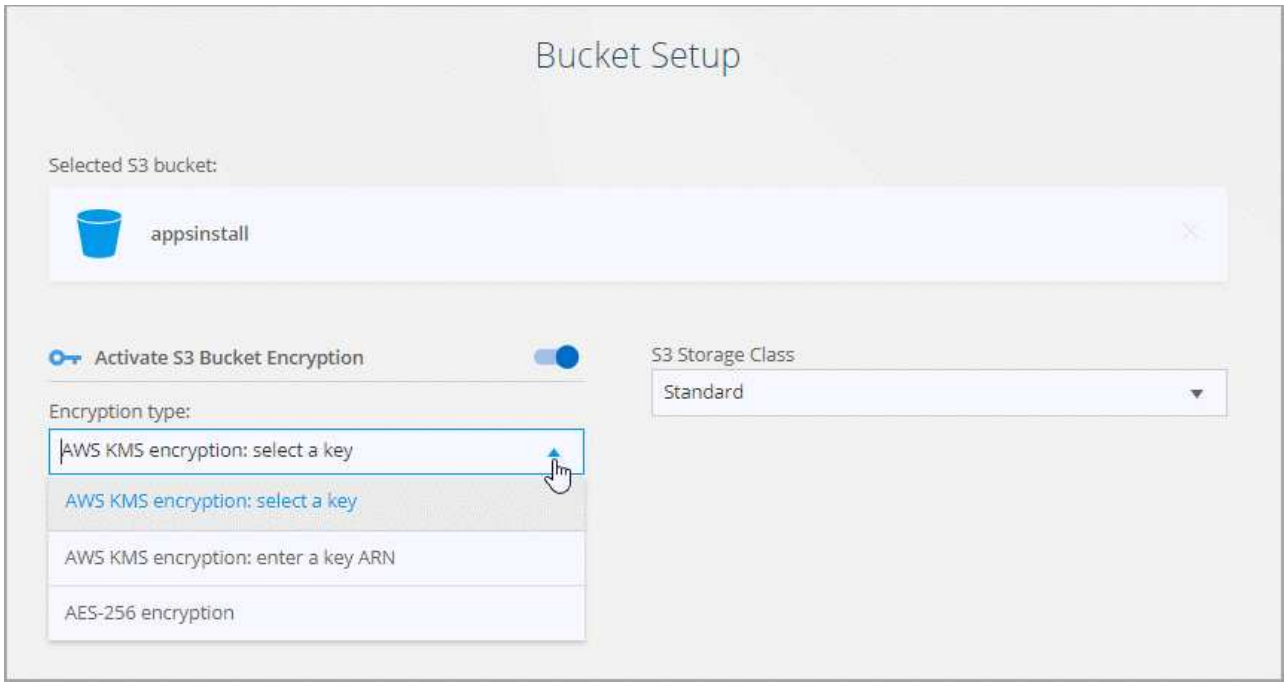
6. 디렉토리 페이지에서 최상위 디렉토리나 하위 디렉토리를 선택하세요.

   복사 및 동기화에서 내보내기를 검색할 수 없는 경우 *수동으로 내보내기 추가*를 선택하고 NFS 내보내기의 이름을 입력합니다.

   NFS 서버에서 두 개 이상의 디렉토리를 동기화하려면 작업을 마친 후 추가 동기화 관계를 만들어야 합니다.

7. **AWS S3** 버킷 페이지에서 버킷을 선택하세요.
   - 버킷 내의 기존 폴더를 선택하거나 버킷 내에 만든 새 폴더를 선택하려면 드릴다운합니다.
   - AWS 계정과 연결되지 않은 S3 버킷을 선택하려면 *목록에 추가*를 선택하세요. "S3 버킷에 특정 권한을 적용해야 합니다." .

8. 버킷 설정 페이지에서 버킷을 설정합니다.
   - S3 버킷 암호화를 활성화할지 선택한 다음 AWS KMS 키를 선택하거나 KMS 키의 ARN을 입력하거나 AES-256 암호화를 선택합니다.
   - S3 스토리지 클래스를 선택하세요. "지원되는 스토리지 클래스 보기" .



9. 설정 페이지에서 소스 파일과 폴더가 대상 위치에서 동기화되고 유지되는 방식을 정의합니다.

일정

향후 동기화를 위해 반복 일정을 선택하거나 동기화 일정을 끕니다. 최대 1분마다 데이터를 동기화하도록 관계를 예약할 수 있습니다.

동기화 시간 초과

동기화가 지정된 분, 시간 또는 일 수 내에 완료되지 않을 경우 복사 및 동기화가 데이터 동기화를 취소해야 하는지 여부를 정의합니다.

알림

NetApp 콘솔의 알림 센터에서 복사 및 동기화 알림을 받을지 여부를 선택할 수 있습니다. 성공적인 데이터 동기화, 실패한 데이터 동기화, 취소된 데이터 동기화에 대한 알림을 활성화할 수 있습니다.

재시도

복사 및 동기화가 파일을 건너뛰기 전에 동기화를 다시 시도해야 하는 횟수를 정의합니다.

연속 동기화

초기 데이터 동기화 후, 복사 및 동기화는 소스 S3 버킷이나 Google Cloud Storage 버킷의 변경 사항을 수신하고 발생하는 모든 변경 사항을 대상에 지속적으로 동기화합니다. 예약된 간격으로 소스를 다시 스캔할 필요가 없습니다.

이 설정은 동기화 관계를 생성할 때와 S3 버킷 또는 Google Cloud Storage에서 Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3 및 StorageGRID 또는 Azure Blob Storage에서 Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS 및 StorageGRID 로 데이터를 동기화할 때만 사용할 수 있습니다.

이 설정을 활성화하면 다음과 같이 다른 기능에 영향을 미칩니다.

- 동기화 일정이 비활성화되었습니다.
- 다음 설정은 기본값으로 돌아갑니다: 동기화 시간 초과, 최근 수정된 파일, 수정 날짜.

- S3가 소스인 경우 크기별 필터는 복사 이벤트에서만 활성화됩니다(삭제 이벤트에서는 활성화되지 않음).
- 관계가 생성된 후에는 관계를 가속화하거나 삭제할 수만 있습니다. 동기화를 중단하거나, 설정을 수정하거나, 보고서를 볼 수 없습니다.

외부 버킷과 지속적인 동기화 관계를 만드는 것이 가능합니다. 그렇게 하려면 다음 단계를 따르세요.

i. 외부 버킷 프로젝트에 대한 Google Cloud 콘솔로 이동합니다.

ii. *클라우드 스토리지 > 설정 > 클라우드 스토리지 서비스 계정*으로 이동합니다.

iii. local.json 파일을 업데이트합니다.

```
{
"protocols": {
    "gcp": {
        "storage-account-email": <storage account email>
}
}
}
```

iv. 데이터 브로커를 다시 시작합니다.

A. sudo pm2 모두 중지

B. sudo pm2 모두 시작

v. 해당 외부 버킷과 지속적인 동기화 관계를 만듭니다.

> 외부 버킷과 지속적인 동기화 관계를 생성하는 데 사용되는 데이터 브로커는 해당 프로젝트의 버킷과 다른 지속적인 동기화 관계를 생성할 수 없습니다.

비교 기준

복사 및 동기화에서 파일이나 디렉토리가 변경되어 다시 동기화해야 하는지 여부를 결정할 때 특정 속성을 비교해야 하는지 여부를 선택합니다.

이러한 속성의 선택을 해제하더라도 복사 및 동기화는 경로, 파일 크기, 파일 이름을 확인하여 소스와 대상을 비교합니다. 변경 사항이 있으면 해당 파일과 디렉토리를 동기화합니다.

다음 속성을 비교하여 복사 및 동기화를 활성화하거나 비활성화할 수 있습니다.

- **mtime**: 파일의 마지막 수정 시간. 이 속성은 디렉토리에 유효하지 않습니다.
- **uid**, **gid**, 및 **mode**: Linux의 권한 플래그입니다.

개체에 대한 복사

이 옵션을 활성화하면 개체 저장소 메타데이터와 태그를 복사할 수 있습니다. 사용자가 소스의 메타데이터를 변경하면 복사 및 동기화는 다음 동기화에서 이 개체를 복사하지만, 사용자가 소스의 태그를 변경하고 데이터 자체는 변경하지 않으면 복사 및 동기화는 다음 동기화에서 개체를 복사하지 않습니다.

관계를 만든 후에는 이 옵션을 편집할 수 없습니다.

태그 복사는 Azure Blob 또는 S3 호환 엔드포인트(S3, StorageGRID 또는 IBM Cloud Object Storage)를 대상으로 포함하는 동기화 관계에서 지원됩니다.

다음 엔드포인트 간의 "클라우드 간" 관계를 통해 메타데이터 복사가 지원됩니다.

- AWS S3
- Azure Blob
- 구글 클라우드 스토리지
- IBM 클라우드 객체 스토리지
- StorageGRID

최근 수정된 파일

예약된 동기화 전에 최근 수정된 파일을 제외하도록 선택합니다.

소스에서 파일 삭제

복사 및 동기화를 통해 파일을 대상 위치로 복사한 후 소스 위치에서 파일을 삭제하도록 선택합니다. 이 옵션을 사용하면 원본 파일이 복사된 후 삭제되므로 데이터 손실 위험이 있습니다.

이 옵션을 활성화하면 데이터 브로커의 local.json 파일에서 매개변수도 변경해야 합니다. 파일을 열고 다음과 같이 업데이트하세요.

```
{
"workers":{
"transferrer":{
"delete-on-source": true
}
}
}
```

local.json 파일을 업데이트한 후에는 다시 시작해야 합니다. `pm2 restart all` .

대상의 파일 삭제

소스에서 파일이 삭제된 경우 대상 위치에서도 파일을 삭제하도록 선택합니다. 기본적으로 대상 위치에서 파일을 삭제하지 않습니다.

파일 유형

각 동기화에 포함할 파일 유형을 정의합니다. 파일, 디렉토리, 심볼릭 링크, 하드 링크입니다.

하드 링크는 보안되지 않은 NFS 간 관계에만 사용할 수 있습니다. 사용자는 하나의 스캐너 프로세스와 하나의 스캐너 동시성으로 제한되며, 스캔은 루트 디렉토리에서 실행해야 합니다.

파일 확장자 제외

동기화에서 제외할 정규식이나 파일 확장자를 지정하려면 파일 확장자를 입력하고 *Enter*를 누릅니다. 예를 들어, *.log 파일을 제외하려면 *log* 또는 _.log_를 입력합니다. 여러 개의 확장자를 사용하는 경우 구분 기호는 필요하지 않습니다. 다음 영상은 짧은 데모를 제공합니다.

동기화 관계에 대한 파일 확장자 제외

정규 표현식은 와일드카드나 글로브 표현식과 다릅니다. 이 기능은 정규 표현식에서만 작동합니다.

디렉토리 제외

이름이나 디렉토리 전체 경로를 입력하고 *Enter*를 눌러 동기화에서 제외할 정규식이나 디렉토리를 최대 15개까지 지정합니다. .copy-offload, .snapshot, ~snapshot 디렉토리는 기본적으로 제외됩니다.

정규 표현식은 와일드카드나 글로브 표현식과 다릅니다. 이 기능은 정규 표현식에서만 작동합니다.

파일 크기

크기에 관계없이 모든 파일을 동기화하거나 특정 크기 범위에 속하는 파일만 동기화하도록 선택합니다.

수정 날짜

마지막 수정 날짜와 관계없이 모든 파일을 선택합니다. 특정 날짜 이후, 특정 날짜 이전 또는 기간 사이에 수정된 파일을 선택합니다.

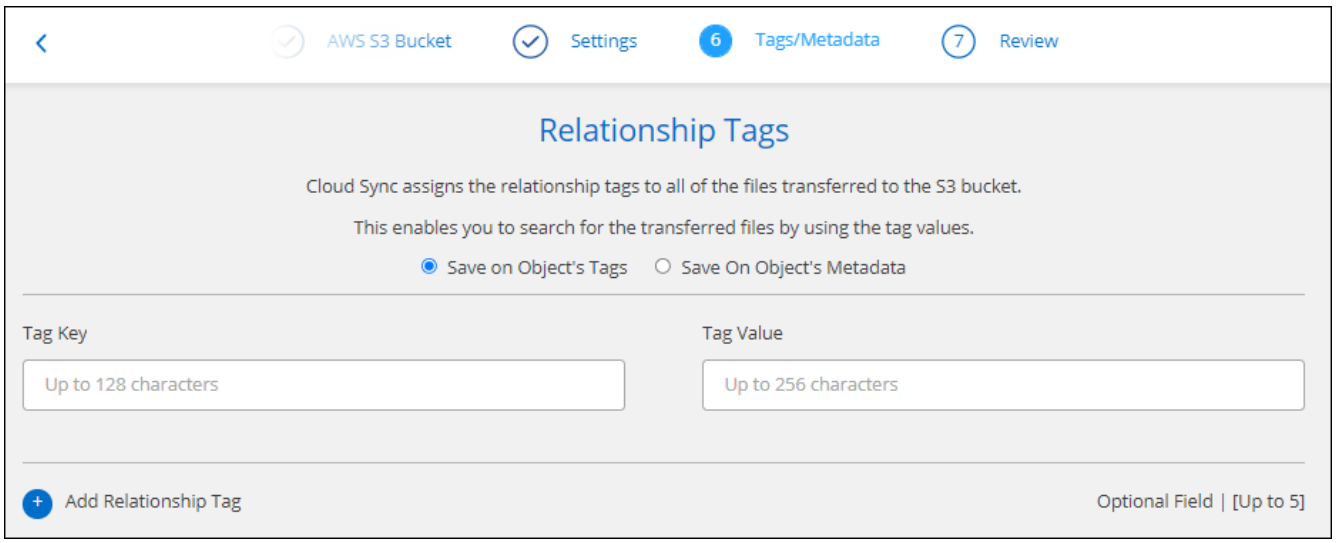
생성 날짜

SMB 서버가 소스인 경우, 이 설정을 사용하면 특정 날짜 이후, 특정 날짜 이전 또는 특정 기간 사이에 생성된 파일을 동기화할 수 있습니다.

ACL - 액세스 제어 목록

관계를 생성할 때 또는 관계를 생성한 후에 설정을 활성화하여 SMB 서버에서 ACL만 복사하거나, 파일만 복사하거나, ACL과 파일을 모두 복사합니다.

10. 태그/메타데이터 페이지에서 S3 버킷으로 전송되는 모든 파일에 태그로 키-값 쌍을 저장할지, 아니면 모든 파일에 메타데이터 키-값 쌍을 할당할지 선택합니다.



StorageGRID 및 IBM Cloud Object Storage에 데이터를 동기화할 때도 동일한 기능을 사용할 수 있습니다. Azure 및 Google Cloud Storage의 경우 메타데이터 옵션만 사용할 수 있습니다.

11. 동기화 관계의 세부 정보를 검토한 다음 *관계 만들기*를 선택합니다.

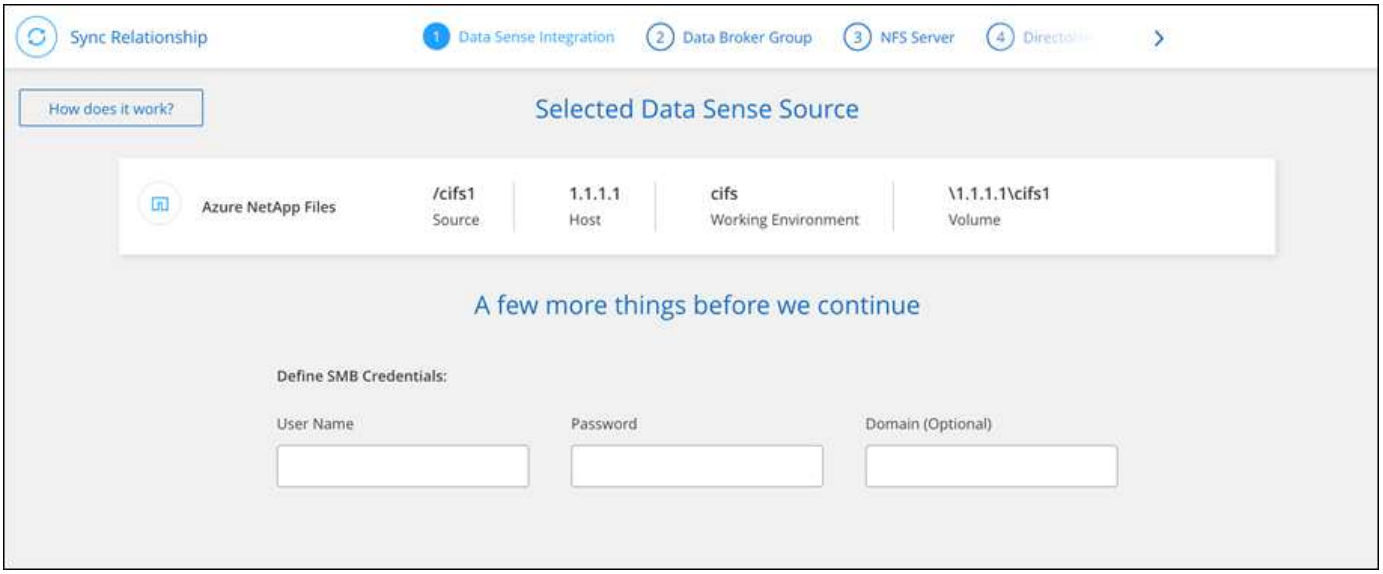
결과

복사 및 동기화는 소스와 대상 간의 데이터 동기화를 시작합니다. 동기화에 걸린 시간, 동기화가 중단되었는지 여부, 복사, 스캔 또는 삭제된 파일 수에 대한 동기화 통계를 사용할 수 있습니다. 그런 다음 다음을 관리할 수 있습니다. "동기화 관계" , "데이터 브로커를 관리하세요" , 또는 "성능과 구성을 최적화하기 위한 보고서 생성" .

NetApp 데이터 분류에서 동기화 관계 만들기

Copy and Sync는 NetApp 데이터 분류와 통합되어 있습니다. NetApp 데이터 분류 내에서 복사 및 동기화를 사용하여 대상 위치로 동기화하려는 소스 파일을 선택할 수 있습니다.

NetApp Data Classification에서 데이터 동기화를 시작하면 모든 소스 정보가 단일 단계에 포함되며 몇 가지 주요 세부 정보만 입력하면 됩니다. 그런 다음 새로운 동기화 관계에 대한 대상 위치를 선택합니다.



"NetApp 데이터 분류에서 동기화 관계를 시작하는 방법을 알아보세요." .

NetApp Copy and Sync에서 SMB 공유의 ACL 복사

NetApp Copy and Sync는 SMB 공유 간, 그리고 SMB 공유와 개체 스토리지(ONTAP S3 제외) 간에 액세스 제어 목록(ACL)을 복사할 수 있습니다. 필요한 경우 robocopy를 사용하여 SMB 공유 간 ACL을 수동으로 보존할 수도 있습니다.

선택

- ACL을 자동으로 복사하도록 복사 및 동기화 설정
- SMB 공유 간 ACL을 수동으로 복사합니다.

ACL을 복사하기 위한 복사 및 동기화 설정

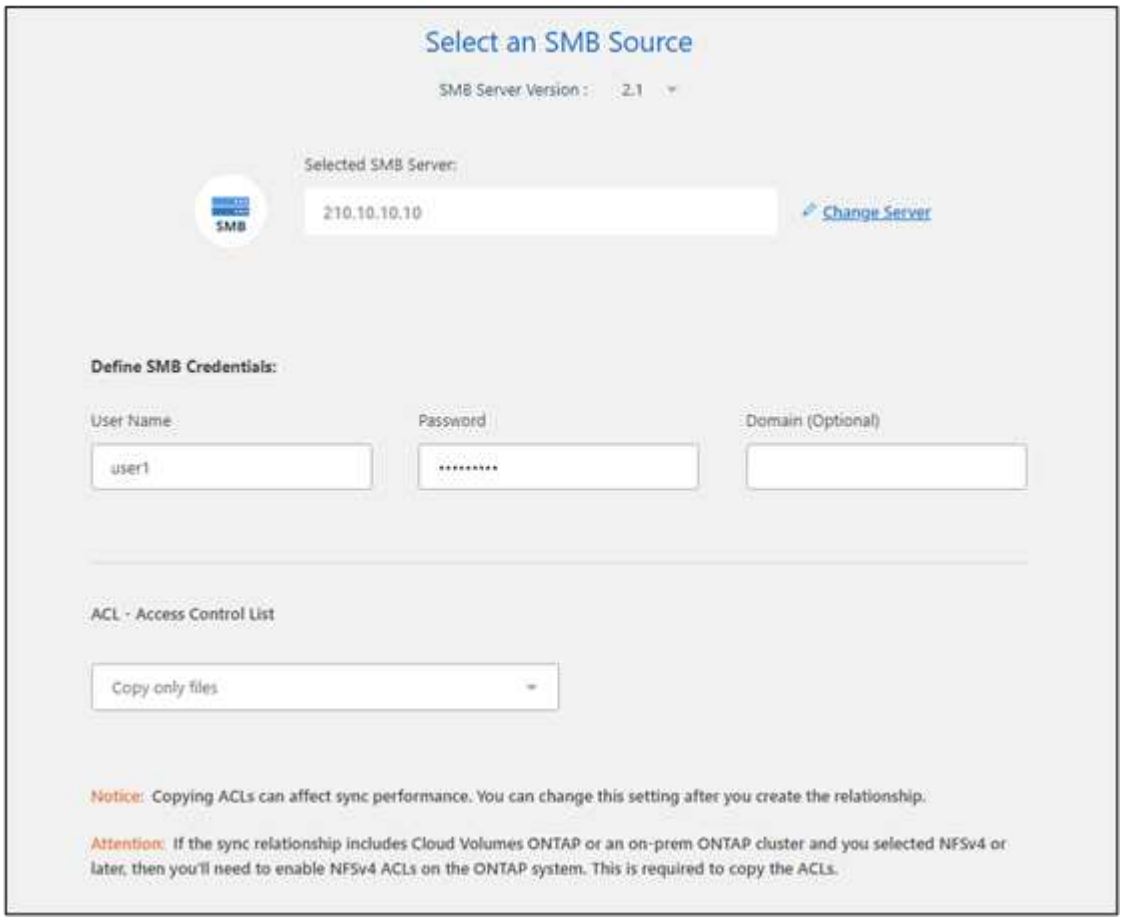
관계를 생성할 때 또는 관계를 생성한 후에 설정을 활성화하여 SMB 공유 간, 그리고 SMB 공유와 개체 스토리지 간에 ACL을 복사합니다.

시작하기 전에

이 기능은 AWS, Azure, Google Cloud Platform 또는 온프레미스 데이터 브로커 등 모든 유형의 데이터 브로커에서 작동합니다. 온프레미스 데이터 브로커는 다음을 실행할 수 있습니다."지원되는 모든 운영 체제" .

새로운 관계를 위한 단계

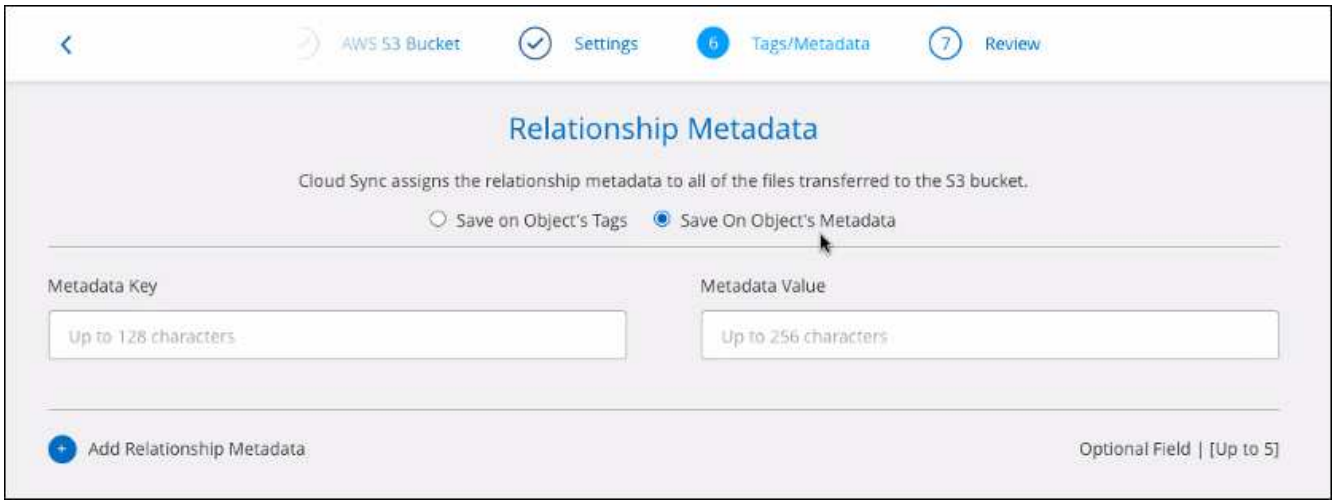
1. "복사 및 동기화에 로그인하세요" .
2. 복사 및 동기화에서 *새 동기화 만들기*를 선택합니다.
3. 소스로 SMB 서버 또는 개체 스토리지를 끌어다 놓고, 대상으로 SMB 서버 또는 개체 스토리지를 끌어다 놓은 다음 *계속*을 선택합니다.
4. **SMB** 서버 페이지에서:
   a. 새로운 SMB 서버를 입력하거나 기존 서버를 선택하고 *계속*을 선택하세요.
   b. SMB 서버에 대한 자격 증명을 입력하세요.
   c. 파일만 복사, **ACL**만 복사, 파일 및 **ACL** 복사 중 하나를 선택하고 *계속*을 선택합니다.



5. 나머지 메시지에 따라 동기화 관계를 만듭니다.

   SMB에서 개체 스토리지로 ACL을 복사할 때 대상에 따라 ACL을 개체의 태그나 개체의 메타데이터에 복사할 수 있습니다. Azure 및 Google Cloud Storage의 경우 메타데이터 옵션만 사용할 수 있습니다.

   다음 스크린샷은 이러한 선택을 할 수 있는 단계의 예를 보여줍니다.



기존 관계에 대한 단계

1. 동기화 관계 위에 마우스를 올려놓고 작업 메뉴를 선택하세요.
2. *설정*을 선택하세요.
3. 파일만 복사, **ACL**만 복사, 파일 및 **ACL** 복사 중 하나를 선택하고 *계속*을 선택합니다.
4. *설정 저장*을 선택하세요.

결과

데이터를 동기화할 때, 복사 및 동기화는 소스와 대상 간의 ACL을 보존합니다.

SMB 공유 간 **ACL**을 수동으로 복사합니다**.**

Windows robocopy 명령을 사용하면 SMB 공유 간의 ACL을 수동으로 보존할 수 있습니다.

단계

1. 두 SMB 공유에 대한 전체 액세스 권한이 있는 Windows 호스트를 식별합니다.
2. 두 엔드포인트 중 하나에 인증이 필요한 경우 **net use** 명령을 사용하여 Windows 호스트에서 엔드포인트에 연결합니다.

   Robocopy를 사용하기 전에 이 단계를 수행해야 합니다.

3. 복사 및 동기화에서 소스 및 대상 SMB 공유 간에 새 관계를 만들거나 기존 관계를 동기화합니다.
4. 데이터 동기화가 완료되면 Windows 호스트에서 다음 명령을 실행하여 ACL과 소유권을 동기화합니다.

   ```
   robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
   /UNILOG:”[logfilepath]
   ```

   _source_와 _target_은 모두 UNC 형식을 사용하여 지정해야 합니다. 예: \\<서버>\<공유>\<경로>

NetApp Copy and Sync에서 전송 중 데이터 암호화를 사용하여 **NFS** 데이터 동기화

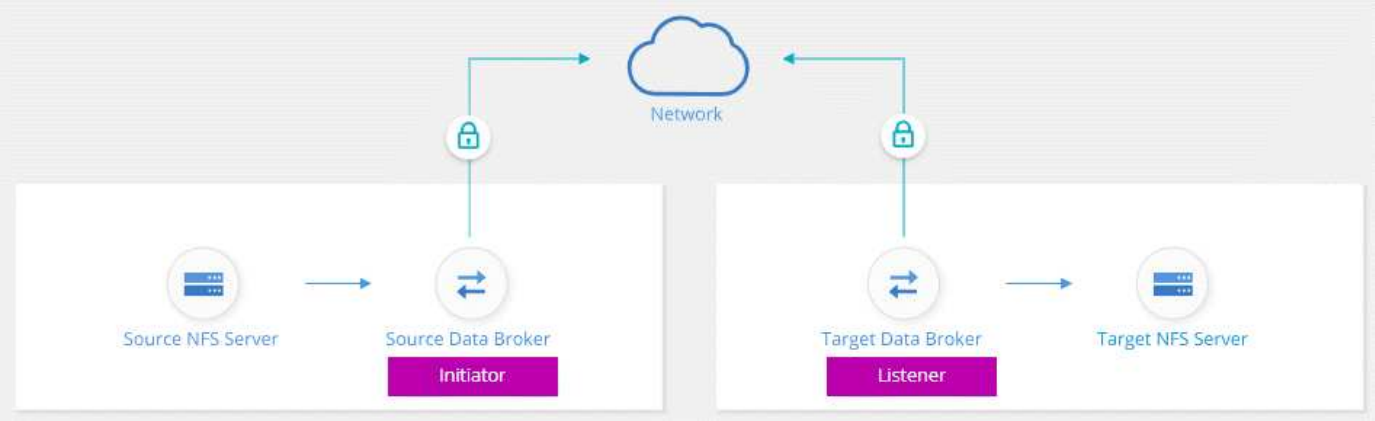
회사에 엄격한 보안 정책이 있는 경우 NetApp Copy and Sync의 전송 중 데이터 암호화를

사용하여 NFS 데이터를 동기화할 수 있습니다. 이 기능은 NFS 서버에서 다른 NFS 서버로, Azure NetApp Files 에서 Azure NetApp Files 로 지원됩니다.

예를 들어, 서로 다른 네트워크에 있는 두 개의 NFS 서버 간에 데이터를 동기화하고 싶을 수 있습니다. 또는 Azure NetApp Files 에서 서브넷이나 지역 간에 데이터를 안전하게 전송해야 할 수도 있습니다.

전송 중인 데이터 암호화 작동 방식

전송 중 데이터 암호화는 두 데이터 브로커 간 네트워크를 통해 전송되는 NFS 데이터를 암호화합니다. 다음 이미지는 두 개의 NFS 서버와 두 개의 데이터 브로커 간의 관계를 보여줍니다.



한 데이터 브로커는 개시자 역할을 합니다. 데이터를 동기화할 시간이 되면 다른 데이터 브로커, 즉 _리스너_에 연결 요청을 보냅니다. 해당 데이터 브로커는 포트 443에서 요청을 수신합니다. 필요한 경우 다른 포트를 사용할 수 있지만, 해당 포트가 다른 서비스에서 사용되고 있지 않은지 확인하세요.

예를 들어, 온프레미스 NFS 서버에서 클라우드 기반 NFS 서버로 데이터를 동기화하는 경우 연결 요청을 수신하는 데이터 브로커와 연결 요청을 보내는 데이터 브로커를 선택할 수 있습니다.

기내 암호화의 작동 방식은 다음과 같습니다.

1. 동기화 관계를 만든 후, 개시자는 다른 데이터 브로커와 암호화된 연결을 시작합니다.
2. 소스 데이터 브로커는 TLS 1.3을 사용하여 소스의 데이터를 암호화합니다.
3. 그런 다음 네트워크를 통해 대상 데이터 브로커로 데이터를 전송합니다.
4. 대상 데이터 브로커는 데이터를 대상에 전송하기 전에 암호를 해독합니다.
5. 최초 복사 후, 복사 및 동기화 기능은 변경된 데이터를 24시간마다 동기화합니다. 동기화할 데이터가 있는 경우, 시작자는 다른 데이터 브로커와 암호화된 연결을 열면서 프로세스가 시작됩니다.

   데이터를 더 자주 동기화하려는 경우"관계를 생성한 후 일정을 변경할 수 있습니다." .

지원되는 **NFS** 버전

- NFS 서버의 경우, 전송 중인 데이터 암호화는 NFS 버전 3, 4.0, 4.1 및 4.2에서 지원됩니다.
- Azure NetApp Files 의 경우 NFS 버전 3 및 4.1에서 전송 중인 데이터 암호화가 지원됩니다.

프록시 서버 제한

암호화된 동기화 관계를 생성하면 암호화된 데이터는 HTTPS를 통해 전송되며 프록시 서버를 통해 라우팅될 수 없습니다.

시작하는 데 필요한 것

다음 사항을 꼭 확인하세요.

- 두 개의 NFS 서버가 충족합니다."소스 및 타겟 요구 사항" 또는 두 개의 서브넷이나 지역에 Azure NetApp Files .
- 서버의 IP 주소 또는 정규화된 도메인 이름입니다.
- 두 데이터 브로커의 네트워크 위치.

  기존 데이터 브로커를 선택할 수 있지만 해당 브로커가 개시자 역할을 해야 합니다. 리스너 데이터 브로커는 새로운 데이터 브로커여야 합니다.

  기존 데이터 브로커 그룹을 사용하려면 그룹에 데이터 브로커가 하나만 있어야 합니다. 그룹 내 여러 데이터 브로커는 암호화된 동기화 관계에서 지원되지 않습니다.

  아직 데이터 브로커를 배포하지 않았다면 데이터 브로커 요구 사항을 검토하세요. 엄격한 보안 정책이 있으므로 포트 443에서의 아웃바운드 트래픽을 포함한 네트워킹 요구 사항을 검토해야 합니다."인터넷 엔드포인트" 데이터 브로커가 연락하는 곳.

  - "AWS 설치 검토"
  - "Azure 설치 검토"
  - "Google Cloud 설치 검토"
  - "Linux 호스트 설치 검토"

데이터 전송 중 암호화를 사용하여 **NFS** 데이터 동기화

두 NFS 서버 간 또는 Azure NetApp Files 간에 새로운 동기화 관계를 만들고, 진행 중 암호화 옵션을 활성화한 다음, 화면의 지시를 따릅니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *새 동기화 만들기*를 선택합니다.
3. *NFS 서버*를 소스 및 대상 위치로 끌어다 놓거나 * Azure NetApp Files*를 소스 및 대상 위치로 끌어다 놓고 *예*를 선택하여 전송 중인 데이터 암호화를 활성화합니다.
4. 다음 지시에 따라 관계를 생성하세요.

   a. **NFS** 서버/* Azure NetApp Files*: NFS 버전을 선택한 다음 새 NFS 소스를 지정하거나 기존 서버를 선택합니다.

   b. 데이터 브로커 기능 정의: 포트에서 연결 요청을 _수신_하는 데이터 브로커와 연결을 _시작_하는 데이터 브로커를 정의합니다. 귀하의 네트워킹 요구 사항에 따라 선택하세요.

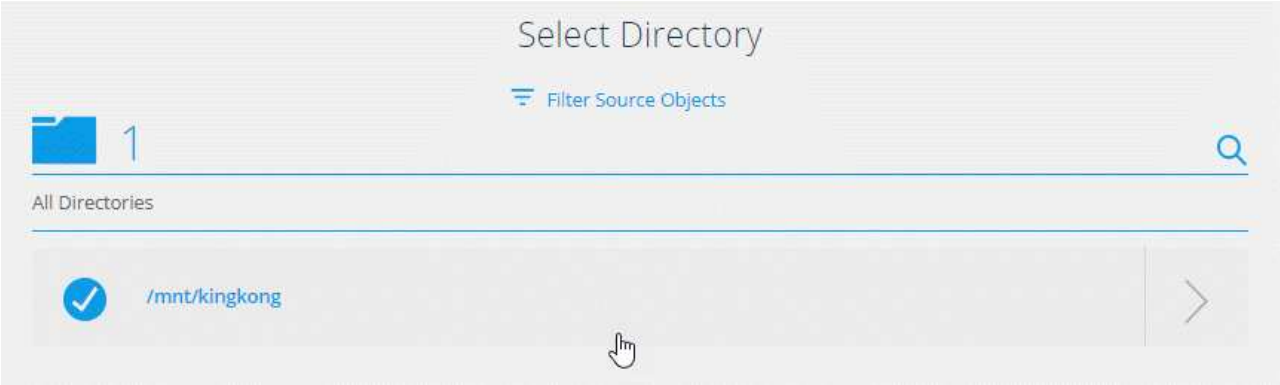
   c. 데이터 브로커: 메시지에 따라 새로운 소스 데이터 브로커를 추가하거나 기존 데이터 브로커를 선택합니다.

      다음 사항에 유의하세요.

- 기존 데이터 브로커 그룹을 사용하려면 그룹에 데이터 브로커가 하나만 있어야 합니다. 그룹 내 여러 데이터 브로커는 암호화된 동기화 관계에서 지원되지 않습니다.
- 소스 데이터 브로커가 리스너 역할을 하는 경우 새로운 데이터 브로커여야 합니다.
- 새로운 데이터 브로커가 필요한 경우 Copy and Sync에서 설치 지침을 안내합니다. 클라우드에 데이터 브로커를 배포하거나 자체 Linux 호스트에 대한 설치 스크립트를 다운로드할 수 있습니다.

d. 디렉토리: 모든 디렉토리를 선택하거나, 드릴다운하여 하위 디렉토리를 선택하여 동기화할 디렉토리를 선택합니다.

*소스 개체 필터링*을 선택하면 소스 파일과 폴더가 대상 위치에서 동기화되고 유지되는 방식을 정의하는 설정을 수정합니다.

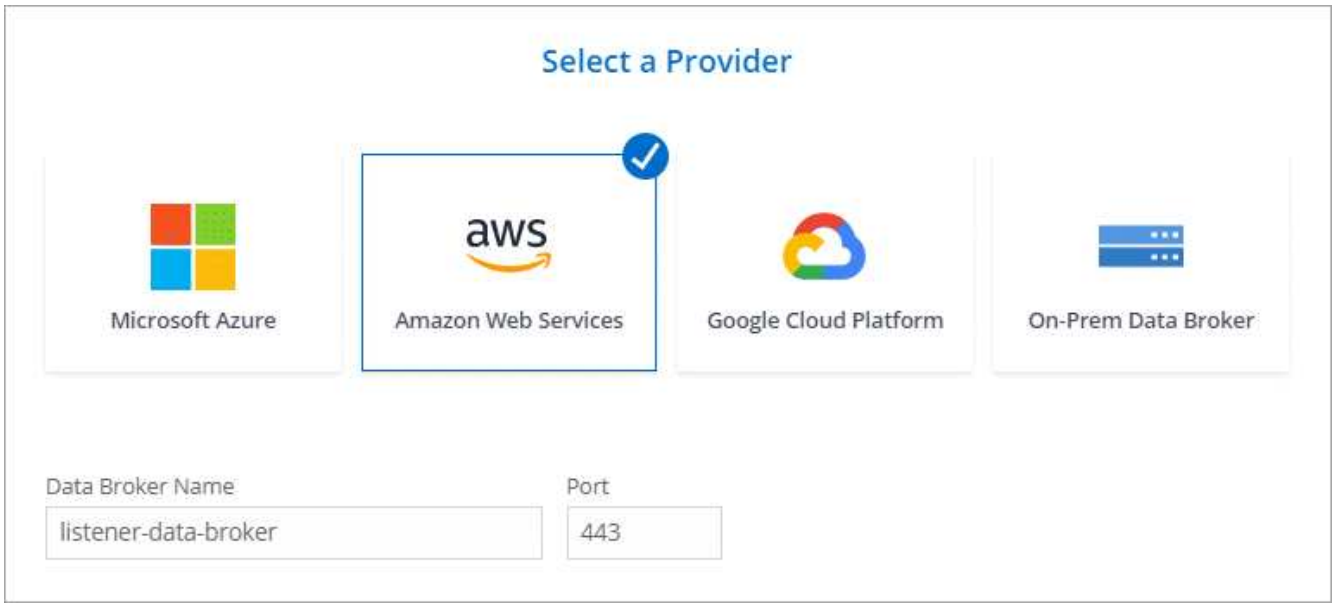


e. 대상 **NFS** 서버/대상 **Azure NetApp Files**: NFS 버전을 선택한 다음 새 NFS 대상을 입력하거나 기존 서버를 선택합니다.

f. 대상 데이터 브로커: 메시지에 따라 새로운 소스 데이터 브로커를 추가하거나 기존 데이터 브로커를 선택합니다.

대상 데이터 브로커가 리스너 역할을 하는 경우 새로운 데이터 브로커여야 합니다.

대상 데이터 브로커가 리스너 역할을 할 때 나타나는 프롬프트의 예는 다음과 같습니다. 포트를 지정하는 옵션에 주목하세요.

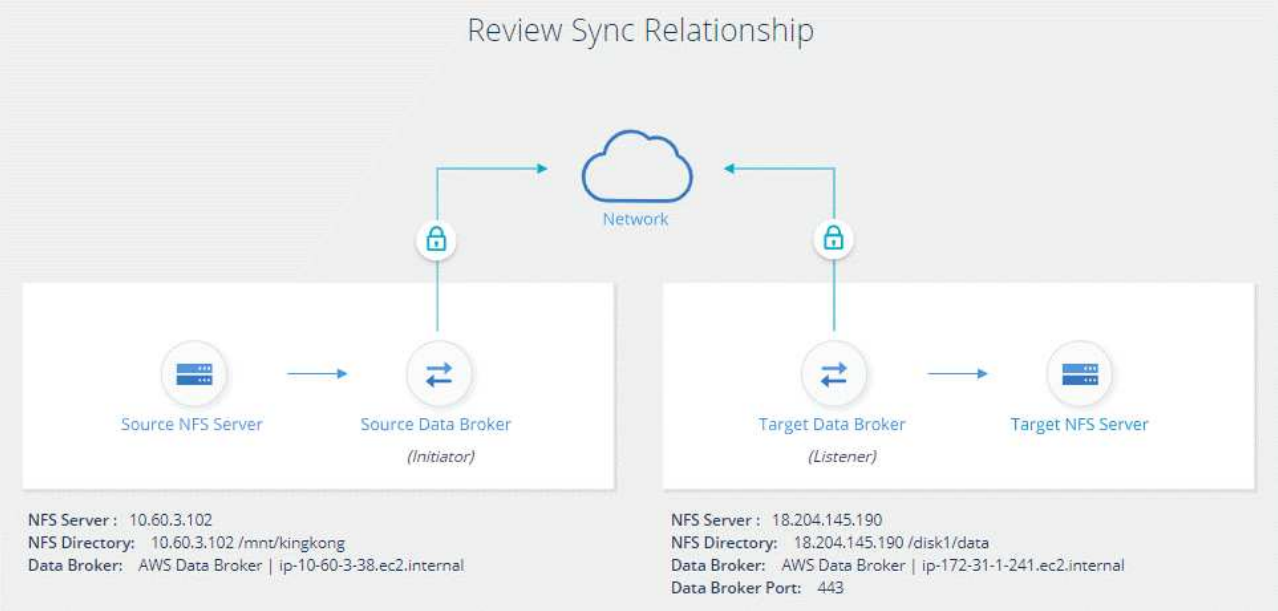


a. 대상 디렉토리: 최상위 디렉토리를 선택하거나, 드릴다운하여 기존 하위 디렉토리를 선택하거나, 내보내기 내에

새 폴더를 만듭니다.

b. 설정: 소스 파일과 폴더가 대상 위치에서 동기화되고 유지되는 방식을 정의합니다.

c. 검토: 동기화 관계의 세부 정보를 검토한 다음 *관계 만들기*를 선택합니다.



결과

복사 및 동기화를 통해 새로운 동기화 관계가 생성됩니다. 완료되면 *대시보드에서 보기*를 선택하여 새 관계에 대한 세부 정보를 확인하세요.

NetApp Copy and Sync에서 외부 HashiCorp Vault를 사용하도록 데이터 브로커 그룹 설정

Amazon S3, Azure 또는 Google Cloud 자격 증명이 필요한 동기화 관계를 만드는 경우 NetApp Copy and Sync 사용자 인터페이스 또는 API를 통해 해당 자격 증명을 지정해야 합니다. 또 다른 방법은 데이터 브로커 그룹을 설정하여 외부 HashiCorp Vault에서 직접 자격 증명(또는 비밀)에 액세스하는 것입니다.

이 기능은 Amazon S3, Azure 또는 Google Cloud 자격 증명이 필요한 동기화 관계를 갖춘 Copy and Sync API를 통해 지원됩니다.

1 금고를 준비하세요

URL을 설정하여 데이터 브로커 그룹에 자격 증명을 제공하도록 볼트를 준비합니다. 보관소의 비밀에 대한 URL은 _Creds_로 끝나야 합니다.

2 데이터 브로커 그룹 준비

그룹의 각 데이터 브로커에 대한 로컬 구성 파일을 수정하여 외부 볼트에서 자격 증명을 가져올 수 있도록 데이터 브로커 그룹을 준비합니다.

3 API를 사용하여 동기화 관계 만들기

이제 모든 것이 설정되었으므로 API 호출을 보내 볼트를 사용하여 비밀을 가져오는 동기화 관계를 만들 수 있습니다.

금고를 준비하세요

보관소에 있는 비밀의 URL을 복사하여 동기화해야 합니다. 해당 URL을 설정하여 볼트를 준비합니다. 만들려는 동기화 관계의 각 소스 및 대상에 대한 자격 증명에 대한 URL을 설정해야 합니다.

URL은 다음과 같이 설정해야 합니다.

```
/<path>/<requestid>/<endpoint-protocol>Creds
```

길
: 비밀에 대한 접두사 경로입니다. 이는 귀하에게만 고유한 값이 될 수 있습니다.

요청 **ID**
: 생성해야 하는 요청 ID입니다. 동기화 관계를 만들 때 API POST 요청의 헤더 중 하나에 ID를 제공해야 합니다.

엔드포인트 프로토콜
: 다음 프로토콜 중 하나, 정의된 대로 "관계 v2 문서 게시" : S3, AZURE 또는 GCP(각각 대문자여야 함).

신용
: URL은 _Creds_로 끝나야 합니다.

예시

다음 예에서는 비밀에 대한 URL을 보여줍니다.

소스 자격 증명에 대한 전체 **URL** 및 경로의 예
: \ http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds 모든 비밀/hb312vdasr2/S3Creds

  예시에서 볼 수 있듯이 접두사 경로는 _/my-path/all-secrets/_이고, 요청 ID는 _hb312vdasr2_이며, 소스 엔드포인트는 S3입니다.

대상 자격 증명에 대한 전체 **URL** 및 경로의 예
: \ http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds 모든 비밀/n32hcbnejk2/AZURECreds

  접두사 경로는 _/my-path/all-secrets/_이고, 요청 ID는 _n32hcbnejk2_이며, 대상 엔드포인트는 Azure입니다.

데이터 브로커 그룹 준비

그룹의 각 데이터 브로커에 대한 로컬 구성 파일을 수정하여 외부 볼트에서 자격 증명을 가져올 수 있도록 데이터 브로커 그룹을 준비합니다.

단계

1. 그룹 내 데이터 브로커에 SSH를 실행합니다.
2. /opt/netapp/databroker/config에 있는 local.json 파일을 편집합니다.

3. enable을 *true*로 설정하고 *external-integrations.hashicorp* 아래의 구성 매개변수 필드를 다음과 같이 설정합니다.

   활성화됨
   - 유효한 값: true/false
   - 유형: 부울
   - 기본값: false
   - 사실: 데이터 브로커는 귀하의 외부 HashiCorp Vault에서 비밀을 얻습니다.
   - 거짓: 데이터 브로커는 로컬 볼트에 자격 증명을 저장합니다.

   URL
   - 유형: 문자열
   - 값: 외부 볼트에 대한 URL

   길
   - 유형: 문자열
   - 값: 자격 증명을 사용하여 비밀에 대한 접두사 경로

   거부-무단
   - 데이터 브로커가 승인되지 않은 외부 볼트를 거부할지 여부를 결정합니다.
   - 유형: 부울
   - 기본값: false

   인증 방법
   - 데이터 브로커가 외부 볼트에서 자격 증명에 액세스하는 데 사용해야 하는 인증 방법
   - 유형: 문자열
   - 유효한 값: "aws-iam" / "role-app" / "gcp-iam"

   역할 이름
   - 유형: 문자열
   - 역할 이름(aws-iam 또는 gcp-iam을 사용하는 경우)

   비밀 **ID** 및 루트 **ID**
   - 유형: 문자열(app-role을 사용하는 경우)

   네임스페이스
   - 유형: 문자열
   - 네임스페이스(필요한 경우 X-Vault-Namespace 헤더)

4. 그룹 내의 다른 데이터 브로커에 대해서도 이 단계를 반복합니다.

aws-role 인증의 예

```
{
          “external-integrations”: {
                  “hashicorp”: {
                          “enabled”: true,
                          “url”: “https://example.vault.com:8200”,
                          “path”: ““my-path/all-secrets”,
                          “reject-unauthorized”: false,
                          “auth-method”: “aws-role”,
                          “aws-role”: {
                                “role-name”: “my-role”
                          }
                  }
        }
}
```

gcp-iam 인증의 예

```
{
"external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": http://ip-10-20-30-55.ec2.internal:8200,
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
"gcp-iam": {
          "role-name": "my-iam-role"
      }
    }
  }
}
```

gcp-iam 인증을 사용할 때 권한 설정

gcp-iam 인증 방법을 사용하는 경우 데이터 브로커에 다음과 같은 GCP 권한이 있어야 합니다.

```
- iam.serviceAccounts.signJwt
```

"데이터 브로커에 대한 GCP 권한 요구 사항에 대해 자세히 알아보세요." .

볼트의 비밀을 사용하여 새로운 동기화 관계 만들기

이제 모든 것이 설정되었으므로 API 호출을 보내 볼트를 사용하여 비밀을 가져오는 동기화 관계를 만들 수 있습니다.

Copy and Sync REST API를 사용하여 관계를 게시합니다.

```
Headers:
Authorization: Bearer <user-token>
Content-Type: application/json
x-account-id: <accountid>
x-netapp-external-request-id-src: request ID as part of path for source
credentials
x-netapp-external-request-id-trg: request ID as part of path for target
credentials
Body: post relationship v2 body
```

- 사용자 토큰과 NetApp 콘솔 계정 ID를 얻으려면"설명서의 이 페이지를 참조하세요" .
- 게시물 관계에 대한 신체를 구축하려면 "관계-v2 API 호출을 참조하세요." .

예

POST 요청의 예:

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik…"
Body:
{
"dataBrokerId": "5e6e111d578dtyuu1555sa60",
"source": {
        "protocol": "s3",
        "s3": {
                "provider": "sgws",
                "host": "1.1.1.1",
                "port": "443",
                "bucket": "my-source"
     },
"target": {
        "protocol": "s3",
        "s3": {
                "bucket": "my-target-bucket"
        }
    }
}
```

NetApp Copy and Sync 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불하세요.

NetApp Copy and Sync의 14일 무료 평가판이 종료된 후에는 동기화 관계에 대한 비용을 두 가지 방법으로 지불할 수 있습니다. 첫 번째 옵션은 AWS 또는 Azure에 가입하여 사용량에 따라 요금을 지불하거나 연간 요금을 지불하는 것입니다. 두 번째 옵션은 NetApp 에서 직접 라이선스를 구매하는 것입니다.

AWS Marketplace나 Azure Marketplace에서 구독할 수 있습니다. 두 곳 모두에서 구독할 수는 없습니다.

마켓플레이스 구독을 통해 NetApp 라이선스를 사용할 수 있습니다. 예를 들어, 동기화 관계가 25개라면 라이선스를 사용하여 처음 20개 동기화 관계에 대한 요금을 지불한 다음, 나머지 5개 동기화 관계에 대해서는 AWS 또는 Azure에서 사용량에 따라 요금을 지불할 수 있습니다.

"라이센스 작동 방식에 대해 자세히 알아보세요" .

무료 체험 기간이 종료된 후 즉시 결제하지 않으면 추가 관계를 생성할 수 없습니다. 기존 관계는 삭제되지 않지만, 구독하거나 라이선스를 입력하기 전까지는 관계를 변경할 수 없습니다.

라이선스는 NetApp Copy and Sync 또는 해당 웹사이트를 통해 관리해야 하며 NetApp 콘솔 구독을 통해서는 관리하지 않습니다.

AWS 구독

AWS를 사용하면 사용량에 따라 비용을 지불하거나 연간으로 지불할 수 있습니다.

사용량에 따른 결제 단계

1. NetApp 콘솔 탐색 메뉴에서 *모빌리티 > 복사 및 동기화*를 선택합니다.
2. *라이선스*를 선택하세요.
3. *AWS*을 선택하세요.
4. *구독*을 선택한 다음 *계속*을 선택하세요.
5. AWS Marketplace에서 구독한 다음 Copy and Sync에 다시 로그인하여 등록을 완료하세요.

   다음 영상은 그 과정을 보여줍니다.

   AWS Marketplace에서 복사 및 동기화 구독

연간 지불 단계

1. "AWS Marketplace 페이지로 이동" .
2. *구독 계속하기*를 선택하세요.
3. 계약 옵션을 선택한 다음 *계약 생성*을 선택하세요.

Azure에서 구독

Azure를 사용하면 사용량에 따라 요금을 지불하거나 연간 요금을 지불할 수 있습니다.

필요한 것

해당 구독에서 기여자 또는 소유자 권한이 있는 Azure 사용자 계정입니다.

단계

1. NetApp 콘솔 탐색 메뉴에서 *모빌리티 > 복사 및 동기화*를 선택합니다.
2. *라이선스*를 선택하세요.
3. *Azure*를 선택하세요.
4. *구독*을 선택한 다음 *계속*을 선택하세요.
5. Azure Portal에서 *만들기*를 선택하고 옵션을 선택한 다음 *구독*을 선택합니다.

   시간당 결제를 원하시면 *월별*을 선택하시고, 1년치를 선불로 결제하려면 *연별*을 선택하세요.

6. 배포가 완료되면 알림 팝업에서 SaaS 리소스 이름을 선택합니다.
7. 복사 및 동기화로 돌아가려면 *계정 구성*을 선택하세요.

   다음 영상은 그 과정을 보여줍니다.

   Azure Marketplace에서 복사 및 동기화 구독

NetApp 에서 라이센스를 구매하고 Copy and Sync에 추가합니다.

동기화 관계에 대한 비용을 선불로 지불하려면 하나 이상의 라이선스를 구매하여 Copy and Sync에 추가해야 합니다.

필요한 것

라이선스의 일련 번호와 라이선스가 연결된 NetApp 지원 사이트 계정의 사용자 이름과 비밀번호가 필요합니다.

단계

1. NetApp 에 문의로 라이선스를 구매하세요.
2. "복사 및 동기화에 로그인하세요" .
3. *라이선스*를 선택하세요.
4. *라이선스 추가*를 선택하고 필요한 정보를 추가하세요.
   a. 일련번호를 입력하세요.
   b. 추가하려는 라이선스와 연결된 NetApp 지원 사이트 계정을 선택하세요.
      - 계정이 이미 NetApp 콘솔에 추가된 경우 드롭다운 목록에서 해당 계정을 선택하세요.
      - 아직 계정이 추가되지 않은 경우 *NSS 자격 증명 추가*를 선택하고 사용자 이름과 비밀번호를 입력한 다음 *등록*을 선택하고 드롭다운 목록에서 해당 계정을 선택하세요.
   c. *추가*를 선택하세요.

라이센스 업데이트

NetApp 에서 구매한 복사 및 동기화 라이선스를 연장한 경우, 새로운 만료 날짜가 복사 및 동기화에서 자동으로 업데이트되지 않습니다. 만료 날짜를 새로 고치려면 라이선스를 다시 추가해야 합니다. 라이선스는 NetApp 콘솔 구독이 아닌 Copy and Sync 또는 해당 웹사이트를 통해 관리해야 합니다.

단계

1. NetApp 콘솔 탐색 메뉴에서 *모빌리티 > 복사 및 동기화*를 선택합니다.
2. *라이선스*를 선택하세요.
3. *라이선스 추가*를 선택하고 필요한 정보를 추가하세요.
   a. 일련번호를 입력하세요.
   b. 추가하려는 라이선스와 연결된 NetApp 지원 사이트 계정을 선택하세요.
   c. *추가*를 선택하세요.

결과

복사 및 동기화는 기존 라이센스를 새로운 만료 날짜로 업데이트합니다.

NetApp Copy and Sync에서 동기화 관계 관리

NetApp Copy and Sync에서 데이터를 즉시 동기화하고, 일정을 변경하는 등 언제든지 동기화 관계를 관리할 수 있습니다.

즉각적인 데이터 동기화를 수행합니다.

다음에 예약된 동기화를 기다리지 않고도 소스와 대상 간에 데이터를 즉시 동기화할 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *대시보드*에서 동기화 관계로 이동하여 다음을 선택합니다. 
3. *지금 동기화*를 선택한 다음 *동기화*를 선택하여 확인합니다.

결과

복사 및 동기화는 관계에 대한 데이터 동기화 프로세스를 시작합니다.

동기화 성능 가속화

관계를 관리하는 그룹에 추가 데이터 브로커를 추가하여 동기화 관계의 성능을 가속화합니다. 추가 데이터 브로커는 새로운 데이터 브로커여야 합니다.

작동 원리

데이터 브로커 그룹이 다른 동기화 관계를 관리하는 경우 그룹에 추가하는 새 데이터 브로커도 해당 동기화 관계의 성능을 가속화합니다.

예를 들어, 세 가지 관계가 있다고 가정해 보겠습니다.

- 관계 1은 데이터 브로커 그룹 A에 의해 관리됩니다.
- 관계 2는 데이터 브로커 그룹 B에서 관리합니다.
- 관계 3은 데이터 브로커 그룹 A에서 관리합니다.

관계 1의 성능을 가속화하기 위해 데이터 브로커 그룹 A에 새로운 데이터 브로커를 추가합니다. 그룹 A는 동기화 관계 3도 관리하므로 관계에 대한 동기화 성능도 자동으로 가속화됩니다.

단계

1. 관계에 있는 기존 데이터 브로커 중 하나 이상이 온라인 상태인지 확인하세요.
2. *대시보드*에서 동기화 관계로 이동하여 다음을 선택합니다. 
3. *가속*을 선택하세요.
4. 화면의 지시에 따라 새로운 데이터 브로커를 생성하세요.

결과

복사 및 동기화는 그룹에 새로운 데이터 브로커를 추가합니다. 다음 데이터 동기화의 성능이 가속화되어야 합니다.

자격 증명 업데이트

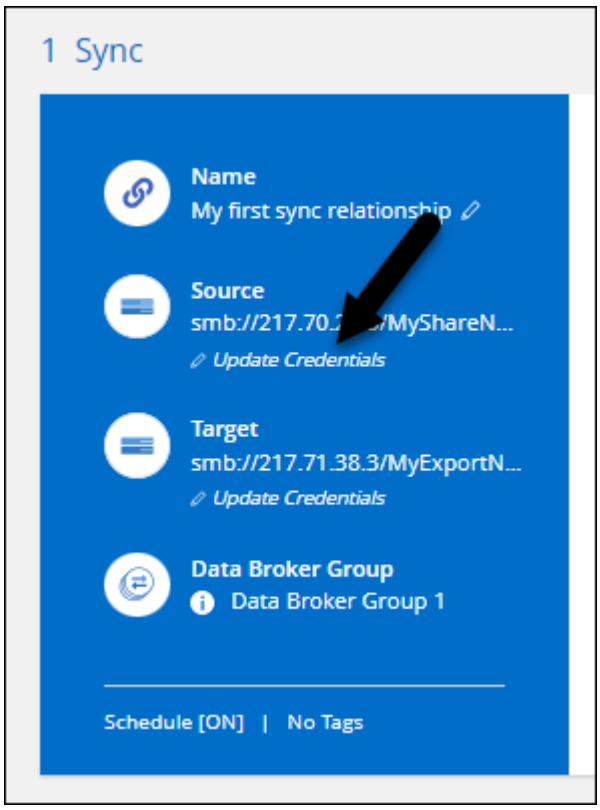
기존 동기화 관계에서 소스 또는 대상의 최신 자격 증명으로 데이터 브로커를 업데이트할 수 있습니다. 보안 정책에 따라 주기적으로 자격 증명을 업데이트해야 하는 경우 자격 증명을 업데이트하면 도움이 될 수 있습니다.

자격 증명 업데이트는 Copy and Sync에 자격 증명이 필요한 모든 소스 또는 대상(Azure Blob, Box, IBM Cloud

Object Storage, StorageGRID, ONTAP S3 Storage, SFTP 및 SMB 서버)에서 지원됩니다.

단계

1. *동기화 대시보드*에서 자격 증명이 필요한 동기화 관계로 이동한 다음 *자격 증명 업데이트*를 선택합니다.



2. 자격 증명을 입력하고 *업데이트*를 선택하세요.

   SMB 서버에 대한 참고 사항: 도메인이 새 것이라면 자격 증명을 업데이트할 때 해당 도메인을 지정해야 합니다. 도메인이 변경되지 않았다면 다시 입력할 필요가 없습니다.

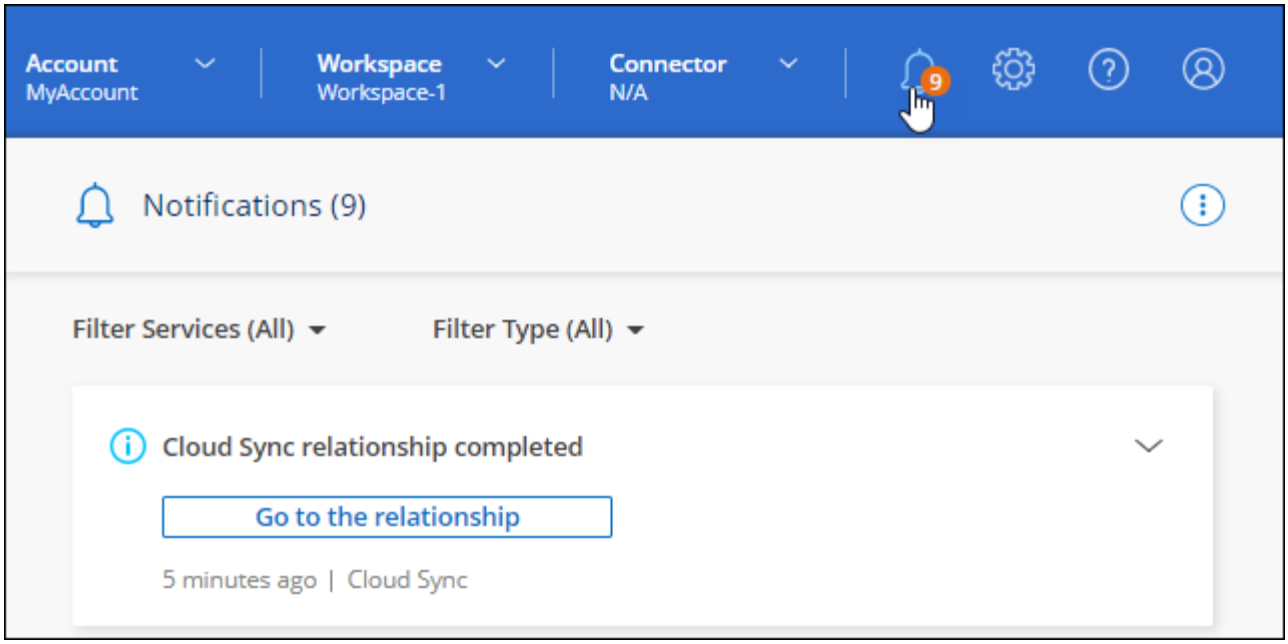
   동기화 관계를 생성할 때 도메인을 입력했지만 자격 증명을 업데이트할 때 새 도메인을 입력하지 않으면 복사 및 동기화는 사용자가 제공한 원래 도메인을 계속 사용합니다.

결과

복사 및 동기화는 데이터 브로커의 자격 증명을 업데이트합니다. 데이터 브로커가 업데이트된 자격 증명을 사용하여 데이터 동기화를 시작할 때까지 최대 10분이 걸릴 수 있습니다.

알림 설정

각 동기화 관계에 대한 알림 설정을 사용하면 NetApp 콘솔의 알림 센터에서 복사 및 동기화 알림을 받을지 여부를 선택할 수 있습니다. 성공적인 데이터 동기화, 실패한 데이터 동기화, 취소된 데이터 동기화에 대한 알림을 활성화할 수 있습니다.



또한, 이메일로 알림을 받으실 수도 있습니다.

단계

1. 동기화 관계에 대한 설정을 수정합니다.
   a. *대시보드*에서 동기화 관계로 이동하여 다음을 선택합니다.
   b. *설정*을 선택하세요.
   c. *알림*을 활성화하세요.
   d. *설정 저장*을 선택하세요.
2. 이메일로 알림을 받으려면 알림 및 알림 설정을 구성하세요.
   a. *설정 > 알림 및 알림 설정*을 선택하세요.
   b. 사용자 한 명 또는 여러 사용자를 선택하고 정보 알림 유형을 선택하세요.
   c. *적용*을 선택하세요.

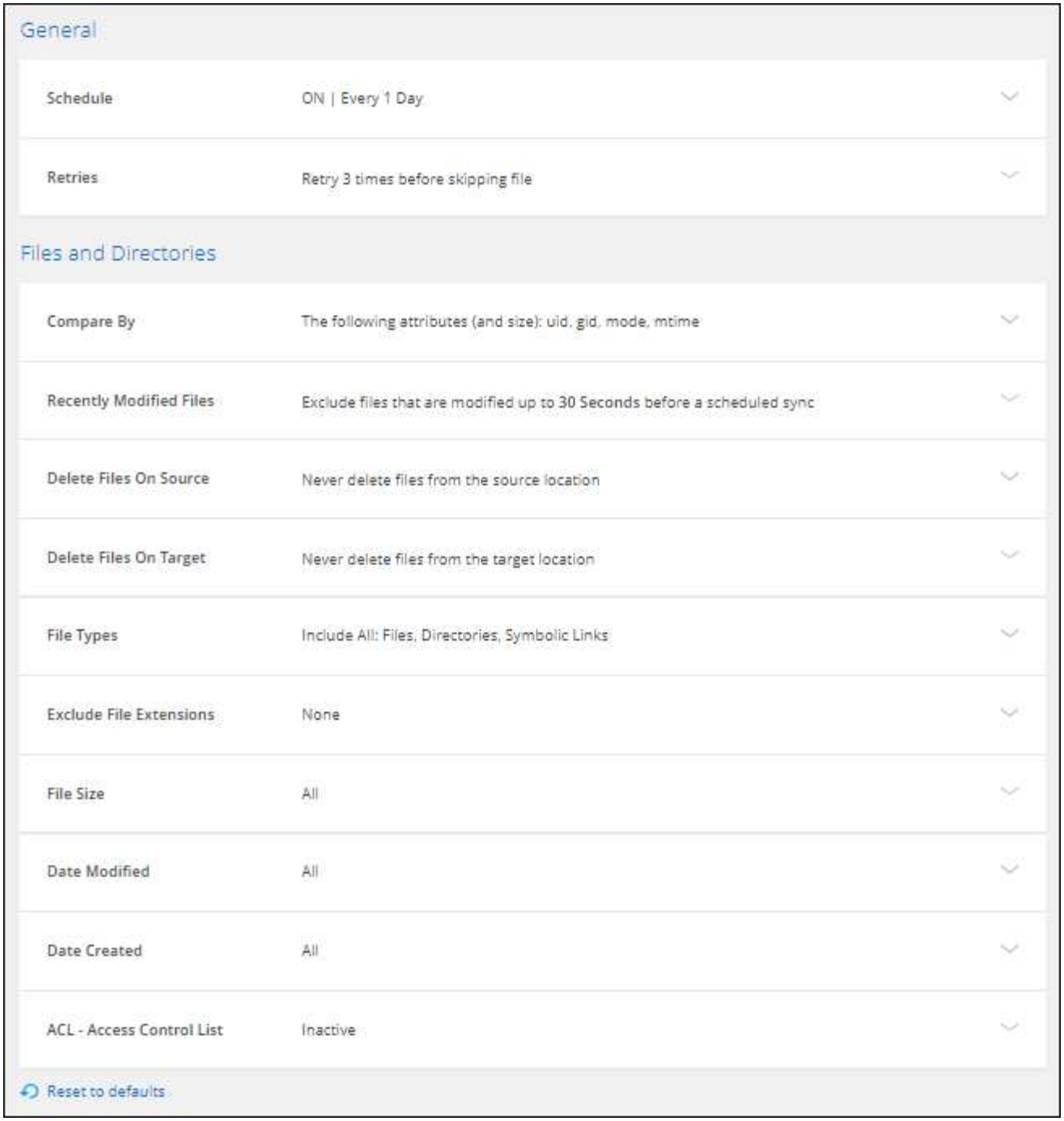
결과

이제 NetApp 콘솔의 알림 센터에서 복사 및 동기화 알림을 받게 되며, 해당 옵션을 구성한 경우 일부 알림은 이메일로 도착합니다.

동기화 관계에 대한 설정 변경

대상 위치에서 소스 파일과 폴더가 동기화되고 유지되는 방식을 정의하는 설정을 수정합니다.

1. *대시보드*에서 동기화 관계로 이동하여 다음을 선택합니다.
2. *설정*을 선택하세요.
3. 설정을 수정합니다.



각 설정에 대한 간략한 설명은 다음과 같습니다.

일정

향후 동기화를 위해 반복 일정을 선택하거나 동기화 일정을 끕니다. 최대 1분마다 데이터를 동기화하도록 관계를 예약할 수 있습니다.

동기화 시간 초과

동기화가 지정된 시간(분, 시간 또는 일) 내에 완료되지 않을 경우 복사 및 동기화가 데이터 동기화를 취소해야 하는지 여부를 정의합니다.

알림

NetApp 콘솔의 알림 센터에서 복사 및 동기화 알림을 받을지 여부를 선택할 수 있습니다. 성공적인 데이터

동기화, 실패한 데이터 동기화, 취소된 데이터 동기화에 대한 알림을 활성화할 수 있습니다.

알림을 받으려면

재시도
: 복사 및 동기화가 파일을 건너뛰기 전에 동기화를 다시 시도해야 하는 횟수를 정의합니다.

비교 기준
: 복사 및 동기화에서 파일이나 디렉토리가 변경되어 다시 동기화해야 하는지 여부를 결정할 때 특정 속성을 비교해야 하는지 여부를 선택합니다.

  이러한 속성의 선택을 해제하더라도 복사 및 동기화는 경로, 파일 크기, 파일 이름을 확인하여 소스와 대상을 비교합니다. 변경 사항이 있으면 해당 파일과 디렉토리를 동기화합니다.

  다음 속성을 비교하여 복사 및 동기화를 활성화하거나 비활성화할 수 있습니다.

  - **mtime**: 파일의 마지막 수정 시간. 이 속성은 디렉토리에 유효하지 않습니다.
  - **uid**, **gid**, 및 **mode**: Linux의 권한 플래그입니다.

개체에 대한 복사
: 관계를 만든 후에는 이 옵션을 편집할 수 없습니다.

최근 수정된 파일
: 예약된 동기화 전에 최근 수정된 파일을 제외하도록 선택합니다.

소스에서 파일 삭제
: 복사 및 동기화를 통해 파일을 대상 위치로 복사한 후 소스 위치에서 파일을 삭제하도록 선택합니다. 이 옵션을 사용하면 원본 파일이 복사된 후 삭제되므로 데이터 손실 위험이 있습니다.

  이 옵션을 활성화하면 데이터 브로커의 local.json 파일에서 매개변수도 변경해야 합니다. 파일을 열고 다음과 같이 업데이트하세요.

```
{
"workers":{
"transferrer":{
"delete-on-source": true
}
}
}
```

  local.json 파일을 업데이트한 후에는 다시 시작해야 합니다. `pm2 restart all` .

대상의 파일 삭제
: 소스에서 파일이 삭제된 경우 대상 위치에서도 파일을 삭제하도록 선택합니다. 기본값은 대상 위치에서 파일을 삭제하지 않는 것입니다.

파일 유형

각 동기화에 포함할 파일 유형을 정의합니다. 파일, 디렉토리, 심볼릭 링크, 하드 링크입니다.

> 하드 링크는 보안되지 않은 NFS 간 관계에만 사용할 수 있습니다. 사용자는 하나의 스캐너 프로세스와 하나의 스캐너 동시성으로 제한되며, 스캔은 루트 디렉토리에서 실행해야 합니다.

파일 확장자 제외

동기화에서 제외할 정규식이나 파일 확장자를 지정하려면 파일 확장자를 입력하고 *Enter*를 누릅니다. 예를 들어, *.log 파일을 제외하려면 *log* 또는 _.log_를 입력합니다. 여러 개의 확장자를 사용하는 경우 구분 기호는 필요하지 않습니다. 다음 영상은 짧은 데모를 제공합니다.

동기화 관계에 대한 파일 확장자 제외

> 정규 표현식은 와일드카드나 글로브 표현식과 다릅니다. 이 기능은 정규 표현식에서만 작동합니다.

디렉토리 제외

이름이나 디렉토리 전체 경로를 입력하고 *Enter*를 눌러 동기화에서 제외할 정규식이나 디렉토리를 최대 15개까지 지정합니다. .copy-offload, .snapshot, ~snapshot 디렉토리는 기본적으로 제외됩니다.

> 정규 표현식은 와일드카드나 글로브 표현식과 다릅니다. 이 기능은 정규 표현식에서만 작동합니다.

파일 크기

크기에 관계없이 모든 파일을 동기화하거나 특정 크기 범위에 속하는 파일만 동기화하도록 선택합니다.

수정 날짜

마지막 수정 날짜와 관계없이 모든 파일을 선택합니다. 특정 날짜 이후, 특정 날짜 이전 또는 기간 사이에 수정된 파일을 선택합니다.

생성 날짜

SMB 서버가 소스인 경우, 이 설정을 사용하면 특정 날짜 이후, 특정 날짜 이전 또는 특정 기간 사이에 생성된 파일을 동기화할 수 있습니다.

ACL - 액세스 제어 목록

관계를 생성할 때 또는 관계를 생성한 후에 설정을 활성화하여 SMB 서버에서 ACL만 복사하거나, 파일만 복사하거나, ACL과 파일을 모두 복사합니다.

4. *설정 저장*을 선택하세요.

결과

복사 및 동기화는 새로운 설정으로 동기화 관계를 수정합니다.

관계 삭제

더 이상 소스와 대상 간에 데이터를 동기화할 필요가 없으면 동기화 관계를 삭제할 수 있습니다. 이 작업은 데이터 브로커 그룹(또는 개별 데이터 브로커 인스턴스)을 삭제하지 않으며 대상에서 데이터를 삭제하지 않습니다.

옵션 **1:** 단일 동기화 관계 삭제

단계

1. *대시보드*에서 동기화 관계로 이동하여 다음을 선택합니다.
2. *삭제*를 선택한 다음 다시 *삭제*를 선택하여 확인합니다.

결과

복사 및 동기화는 동기화 관계를 삭제합니다.

옵션 **2:** 여러 동기화 관계 삭제

단계

1. *대시보드*에서 "새 동기화 만들기" 버튼으로 이동하여 선택하세요.
2. 삭제하려는 동기화 관계를 선택하고, *삭제*를 선택한 다음, 다시 *삭제*를 선택하여 확인합니다.

결과

복사 및 동기화는 동기화 관계를 삭제합니다.

NetApp Copy and Sync에서 데이터 브로커 그룹 관리

NetApp Copy and Sync의 데이터 브로커 그룹은 소스 위치에서 대상 위치로 데이터를 동기화합니다. 생성하는 각 동기화 관계에는 그룹에 하나 이상의 데이터 브로커가 필요합니다. 그룹에 새로운 데이터 브로커를 추가하고, 그룹에 대한 정보를 보는 등 데이터 브로커 그룹을 관리합니다.

데이터 브로커 그룹의 작동 방식

데이터 브로커 그룹에는 하나 이상의 데이터 브로커가 포함될 수 있습니다. 데이터 브로커를 그룹화하면 동기화 관계의 성능을 개선하는 데 도움이 될 수 있습니다.

그룹은 여러 관계를 관리할 수 있습니다.

데이터 브로커 그룹은 한 번에 하나 이상의 동기화 관계를 관리할 수 있습니다.

예를 들어, 세 가지 관계가 있다고 가정해 보겠습니다.

- 관계 1은 데이터 브로커 그룹 A에 의해 관리됩니다.
- 관계 2는 데이터 브로커 그룹 B에서 관리합니다.
- 관계 3은 데이터 브로커 그룹 A에서 관리합니다.

관계 1의 성능을 가속화하기 위해 데이터 브로커 그룹 A에 새로운 데이터 브로커를 추가합니다. 그룹 A는 동기화 관계 3도 관리하므로 관계에 대한 동기화 성능도 자동으로 가속화됩니다.

그룹 내 데이터 브로커 수

많은 경우, 단일 데이터 브로커가 동기화 관계에 대한 성능 요구 사항을 충족할 수 있습니다. 그렇지 않은 경우 그룹에 추가 데이터 브로커를 추가하여 동기화 성능을 가속화할 수 있습니다. 하지만 먼저 동기화 성능에 영향을 줄 수 있는 다른 요소를 확인해야 합니다. "여러 데이터 브로커가 필요한 경우를 결정하는 방법에 대해 자세히 알아보세요." .

보안 권장 사항

데이터 브로커 머신의 보안을 보장하기 위해 NetApp 다음을 권장합니다.

- SSH는 X11 전달을 허용해서는 안 됩니다.
- SSH는 TCP 연결 전달을 허용해서는 안 됩니다.
- SSH는 터널을 허용해서는 안 됩니다.
- SSH는 클라이언트 환경 변수를 허용해서는 안 됩니다.

이러한 보안 권장 사항은 데이터 브로커 시스템에 대한 무단 연결을 방지하는 데 도움이 될 수 있습니다.

그룹에 새로운 데이터 브로커 추가

새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다.

- 새로운 동기화 관계를 생성할 때

  "동기화 관계를 생성할 때 새 데이터 브로커를 만드는 방법을 알아보세요." .

- 데이터 브로커 관리 페이지에서 *새 데이터 브로커 추가*를 선택하면 새 그룹에 데이터 브로커가 생성됩니다.
- 기존 그룹에서 새 데이터 브로커를 만들어 데이터 브로커 관리 페이지에서

시작하기 전에

- 암호화된 동기화 관계를 관리하는 그룹에 데이터 브로커를 추가할 수 없습니다.
- 기존 그룹에서 데이터 브로커를 만들려면 해당 데이터 브로커가 온프레미스 데이터 브로커이거나 동일한 유형의 데이터 브로커여야 합니다.

  예를 들어, 그룹에 AWS 데이터 브로커가 포함되어 있는 경우 해당 그룹에서 AWS 데이터 브로커나 온프레미스 데이터 브로커를 만들 수 있습니다. Azure 데이터 브로커나 Google Cloud 데이터 브로커는 동일한 데이터 브로커 유형이 아니므로 만들 수 없습니다.

새 그룹에서 데이터 브로커를 만드는 단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. *새로운 데이터 브로커 추가*를 선택하세요.
4. 화면의 지시에 따라 데이터 브로커를 생성하세요.

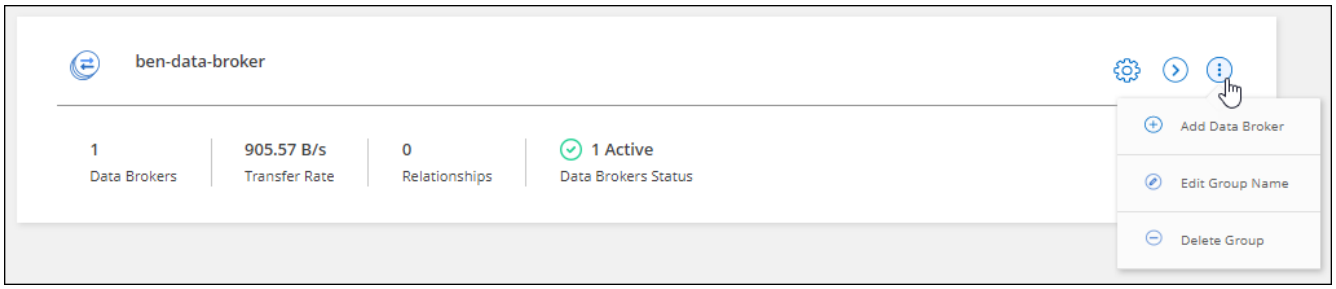
   도움이 필요하면 다음 페이지를 참조하세요.

   - "AWS에서 데이터 브로커 만들기"

- "Azure에서 데이터 브로커 만들기"
- "Google Cloud에서 데이터 브로커 만들기"
- "Linux 호스트에 데이터 브로커 설치"

기존 그룹에서 데이터 브로커를 만드는 단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. 작업 메뉴를 선택하고 *데이터 브로커 추가*를 선택합니다.



4. 메시지에 따라 그룹에서 데이터 브로커를 만듭니다.

   도움이 필요하면 다음 페이지를 참조하세요.

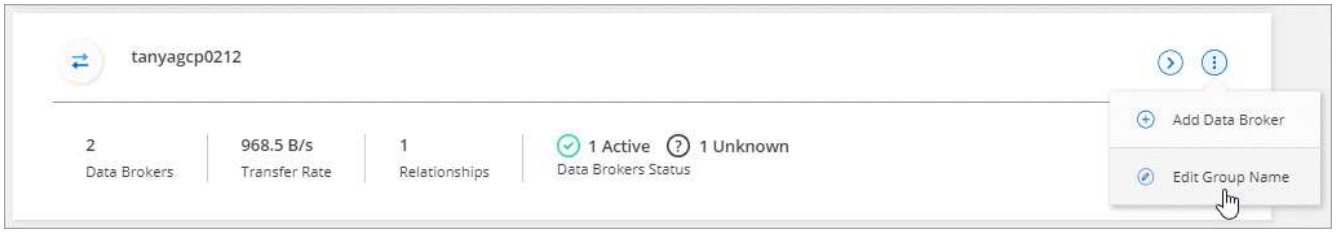
   - "AWS에서 데이터 브로커 만들기"
   - "Azure에서 데이터 브로커 만들기"
   - "Google Cloud에서 데이터 브로커 만들기"
   - "Linux 호스트에 데이터 브로커 설치"

그룹 이름 편집

언제든지 데이터 브로커 그룹의 이름을 변경할 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. 작업 메뉴를 선택하고 *그룹 이름 편집*을 선택하세요.



4. 새 이름을 입력하고 *저장*을 선택하세요.

결과

복사 및 동기화는 데이터 브로커 그룹의 이름을 업데이트합니다.

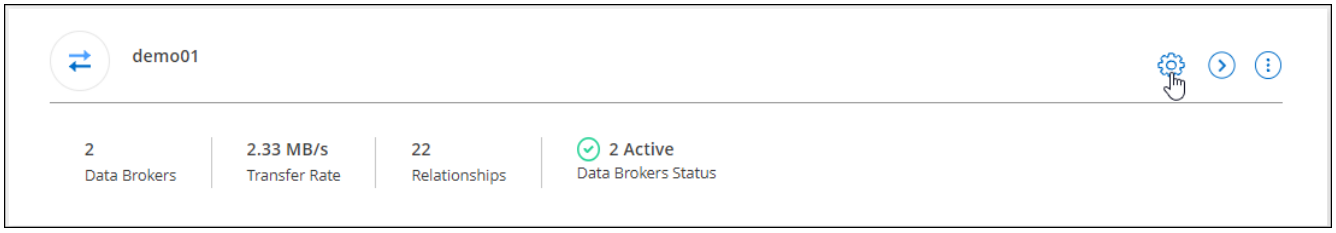
통합 구성 설정

동기화 프로세스 중에 동기화 관계에 오류가 발생하는 경우, 데이터 브로커 그룹의 동시성을 통합하면 동기화 오류 수를 줄이는 데 도움이 될 수 있습니다. 그룹 구성을 변경하면 전송 속도가 느려져 성능에 영향을 미칠 수 있습니다.

구성을 직접 변경하는 것은 권장하지 않습니다. 구성을 언제 변경해야 하는지, 어떻게 변경해야 하는지 알아보려면 NetApp 에 문의하세요.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *데이터 브로커 관리*를 선택하세요.
3. 데이터 브로커 그룹에 대한 설정 아이콘을 선택합니다.



4. 필요에 따라 설정을 변경한 다음 *구성 통합*을 선택합니다.

   다음 사항에 유의하세요.

   - 어떤 설정을 변경할지 선택할 수 있습니다. 네 가지 설정을 모두 한꺼번에 변경할 필요는 없습니다.
   - 새로운 구성이 데이터 브로커로 전송되면 데이터 브로커가 자동으로 다시 시작되어 새로운 구성을 사용합니다.
   - 이 변경 사항이 적용되어 복사 및 동기화 인터페이스에 표시될 때까지 최대 1분이 걸릴 수 있습니다.
   - 데이터 브로커가 실행 중이 아니면 Copy and Sync가 통신할 수 없기 때문에 구성이 변경되지 않습니다. 데이터 브로커가 다시 시작되면 구성이 변경됩니다.
   - 통합 구성을 설정하면 모든 새로운 데이터 브로커가 자동으로 새 구성을 사용합니다.

그룹 간 데이터 브로커 이동

대상 데이터 브로커 그룹의 성능을 가속화해야 하는 경우 데이터 브로커를 한 그룹에서 다른 그룹으로 이동합니다.

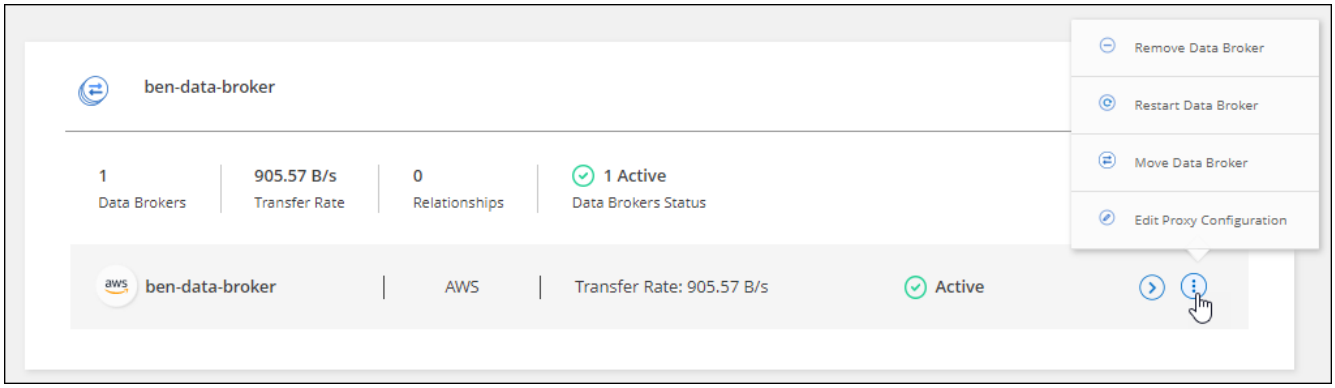
예를 들어, 데이터 브로커가 더 이상 동기화 관계를 관리하지 않는 경우 동기화 관계를 관리하는 다른 그룹으로 쉽게 이동할 수 있습니다.

제한 사항

- 데이터 브로커 그룹이 동기화 관계를 관리하고 그룹에 데이터 브로커가 하나뿐인 경우 해당 데이터 브로커를 다른 그룹으로 이동할 수 없습니다.
- 암호화된 동기화 관계를 관리하는 그룹으로 데이터 브로커를 이동할 수 없습니다.
- 현재 배포 중인 데이터 브로커는 이동할 수 없습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. 선택하다 그룹 내 데이터 브로커 목록을 확장합니다.
4. 데이터 브로커의 작업 메뉴를 선택하고 *데이터 브로커 이동*을 선택합니다.



5. 새로운 데이터 브로커 그룹을 만들거나 기존 데이터 브로커 그룹을 선택하세요.
6. *이동*을 선택하세요.

결과

복사 및 동기화는 데이터 브로커를 새 데이터 브로커 그룹이나 기존 데이터 브로커 그룹으로 이동합니다. 이전 그룹에 다른 데이터 브로커가 없는 경우 복사 및 동기화는 해당 그룹을 삭제합니다.

프록시 구성 업데이트

새로운 프록시 구성에 대한 세부 정보를 추가하거나 기존 프록시 구성을 편집하여 데이터 브로커의 프록시 구성을 업데이트합니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. 선택하다 그룹 내 데이터 브로커 목록을 확장합니다.
4. 데이터 브로커의 작업 메뉴를 선택하고 *프록시 구성 편집*을 선택합니다.
5. 프록시에 대한 세부 정보를 지정합니다: 호스트 이름, 포트 번호, 사용자 이름, 비밀번호.
6. *업데이트*를 선택하세요.

결과

복사 및 동기화는 인터넷 액세스를 위해 프록시 구성을 사용하도록 데이터 브로커를 업데이트합니다.

데이터 브로커 구성 보기

데이터 브로커의 호스트 이름, IP 주소, 사용 가능한 CPU 및 RAM 등을 파악하기 위해 해당 브로커에 대한 세부 정보를 보고 싶을 수 있습니다.

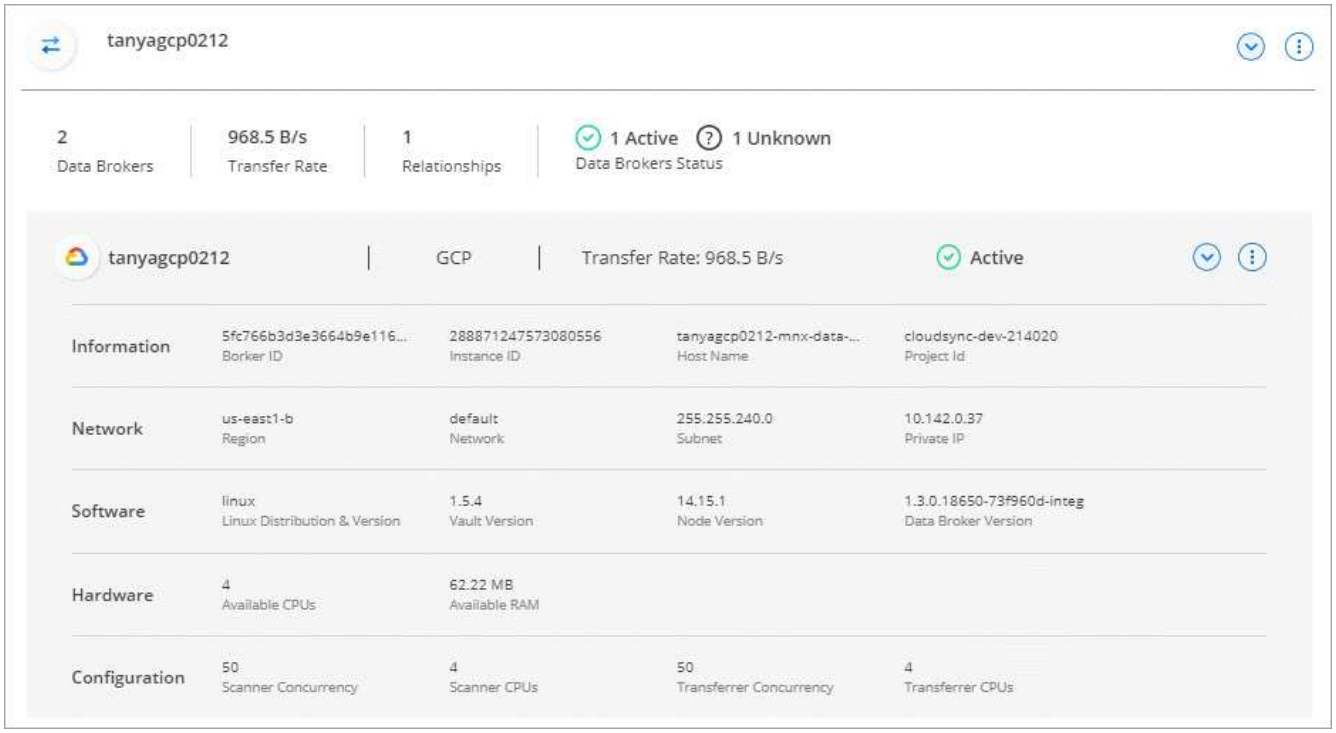
Copy and Sync는 데이터 브로커에 대한 다음과 같은 세부 정보를 제공합니다.

- 기본 정보: 인스턴스 ID, 호스트 이름 등
- 네트워크: 지역, 네트워크, 서브넷, 개인 IP 등
- 소프트웨어: Linux 배포판, 데이터 브로커 버전 등
- 하드웨어: CPU 및 RAM
- 구성: 데이터 브로커의 두 가지 주요 프로세스(스캐너 및 전송기)에 대한 세부 정보

> 스캐너는 소스와 타겟을 스캔하여 무엇을 복사해야 할지 결정합니다. 전송자는 실제로 복사를 수행합니다. NetApp 담당자는 이러한 구성 세부 정보를 사용하여 성능을 최적화할 수 있는 작업을 제안할 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. 선택하다 그룹 내 데이터 브로커 목록을 확장합니다.
4. 선택하다 데이터 브로커에 대한 세부 정보를 보려면.



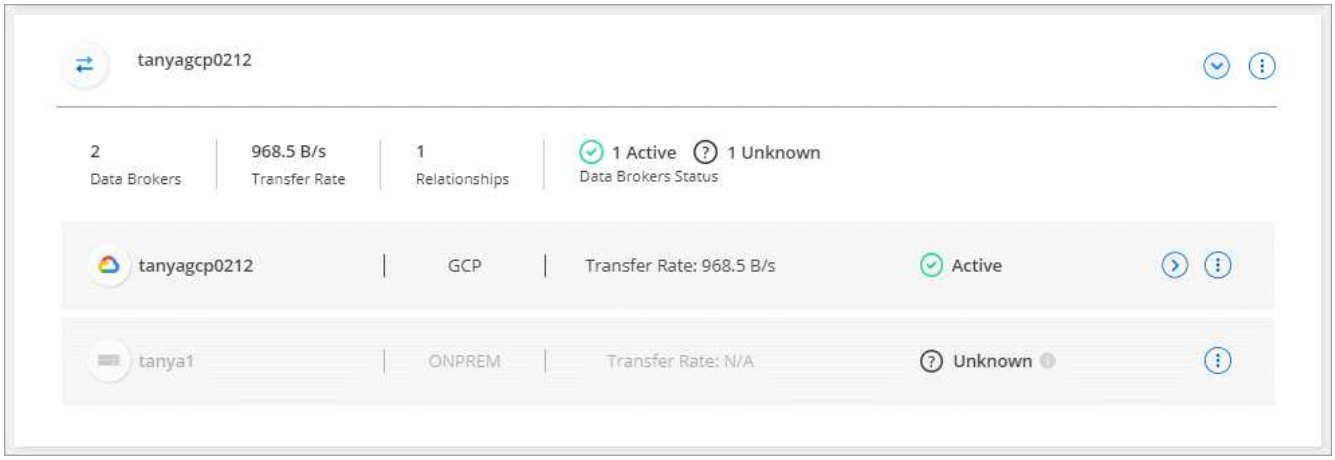
데이터 브로커와 문제 해결

복사 및 동기화는 문제 해결에 도움이 되는 각 데이터 브로커의 상태를 표시합니다.

단계

1. "복사 및 동기화에 로그인하세요" .

2. "알 수 없음" 또는 "실패" 상태인 데이터 브로커를 식별합니다.



3. 위에 마우스를 올려 놓으세요 실패 이유를 보려면 아이콘을 클릭하세요.
4. 문제를 해결하세요.

   예를 들어, 데이터 브로커가 오프라인인 경우 간단히 다시 시작해야 할 수도 있고, 초기 배포에 실패한 경우 데이터 브로커를 제거해야 할 수도 있습니다.

그룹에서 데이터 브로커 제거

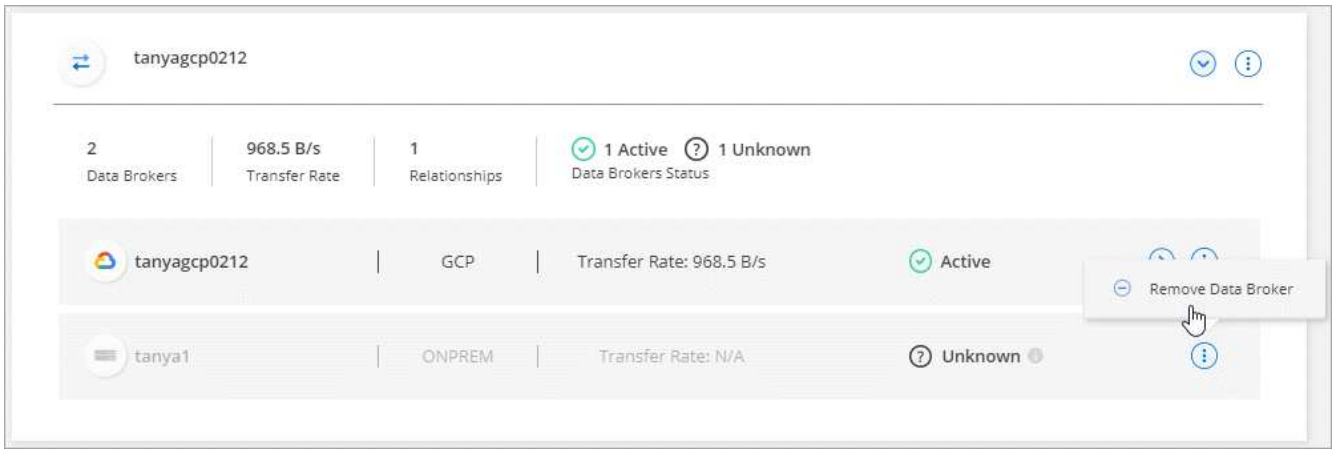
더 이상 필요하지 않거나 초기 배포에 실패한 경우 그룹에서 데이터 브로커를 제거할 수 있습니다. 이 작업을 수행하면 Copy and Sync 레코드에서 데이터 브로커만 삭제됩니다. 데이터 브로커와 추가 클라우드 리소스를 직접 수동으로 삭제해야 합니다.

당신이 알아야 할 것들

- 복사 및 동기화는 그룹에서 마지막 데이터 브로커를 제거하면 그룹을 삭제합니다.
- 해당 그룹을 사용하는 관계가 있는 경우, 해당 그룹에서 마지막 데이터 브로커를 제거할 수 없습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. 선택하다 그룹 내 데이터 브로커 목록을 확장합니다.
4. 데이터 브로커에 대한 작업 메뉴를 선택하고 *데이터 브로커 제거*를 선택합니다.



5. *데이터 브로커 제거*를 선택하세요.

결과

복사 및 동기화를 수행하면 그룹에서 데이터 브로커가 제거됩니다.

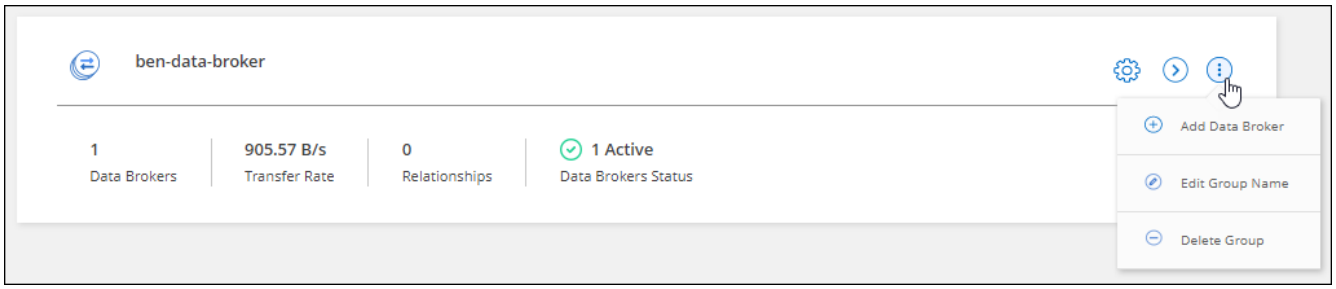
데이터 브로커 그룹 삭제

데이터 브로커 그룹이 더 이상 동기화 관계를 관리하지 않는 경우 그룹을 삭제하면 모든 데이터 브로커가 복사 및 동기화에서 제거됩니다.

Copy and Sync에서 제거한 데이터 브로커는 Copy and Sync의 레코드에서만 삭제됩니다. 클라우드 공급자와 추가 클라우드 리소스에서 데이터 브로커 인스턴스를 수동으로 삭제해야 합니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 데이터 브로커 관리*를 선택합니다.
3. 작업 메뉴를 선택하고 *그룹 삭제*를 선택하세요.



4. 확인하려면 그룹 이름을 입력하고 *그룹 삭제*를 선택하세요.

결과

복사 및 동기화는 데이터 브로커를 제거하고 그룹을 삭제합니다.

NetApp Copy and Sync에서 구성을 조정하기 위한 보고서를 만들고 봅니다.

NetApp Copy and Sync에서 보고서를 만들고 확인하여 NetApp 직원의 도움을 받아 데이터 브로커의 구성을 조정하고 성능을 개선하는 데 사용할 수 있는 정보를 얻으세요.

각 보고서는 동기화 관계의 경로에 대한 심층적인 세부 정보를 제공합니다. 여기에는 디렉토리, 파일, 심볼릭 링크의 수, 파일 크기의 분포, 디렉토리의 깊이와 너비, 수정 시간, 액세스 시간이 포함됩니다. 이는 대시보드에서 사용할 수 있는 동기화 통계와 다릅니다. "동기화를 성공적으로 생성하고 완료" .

보고서 만들기

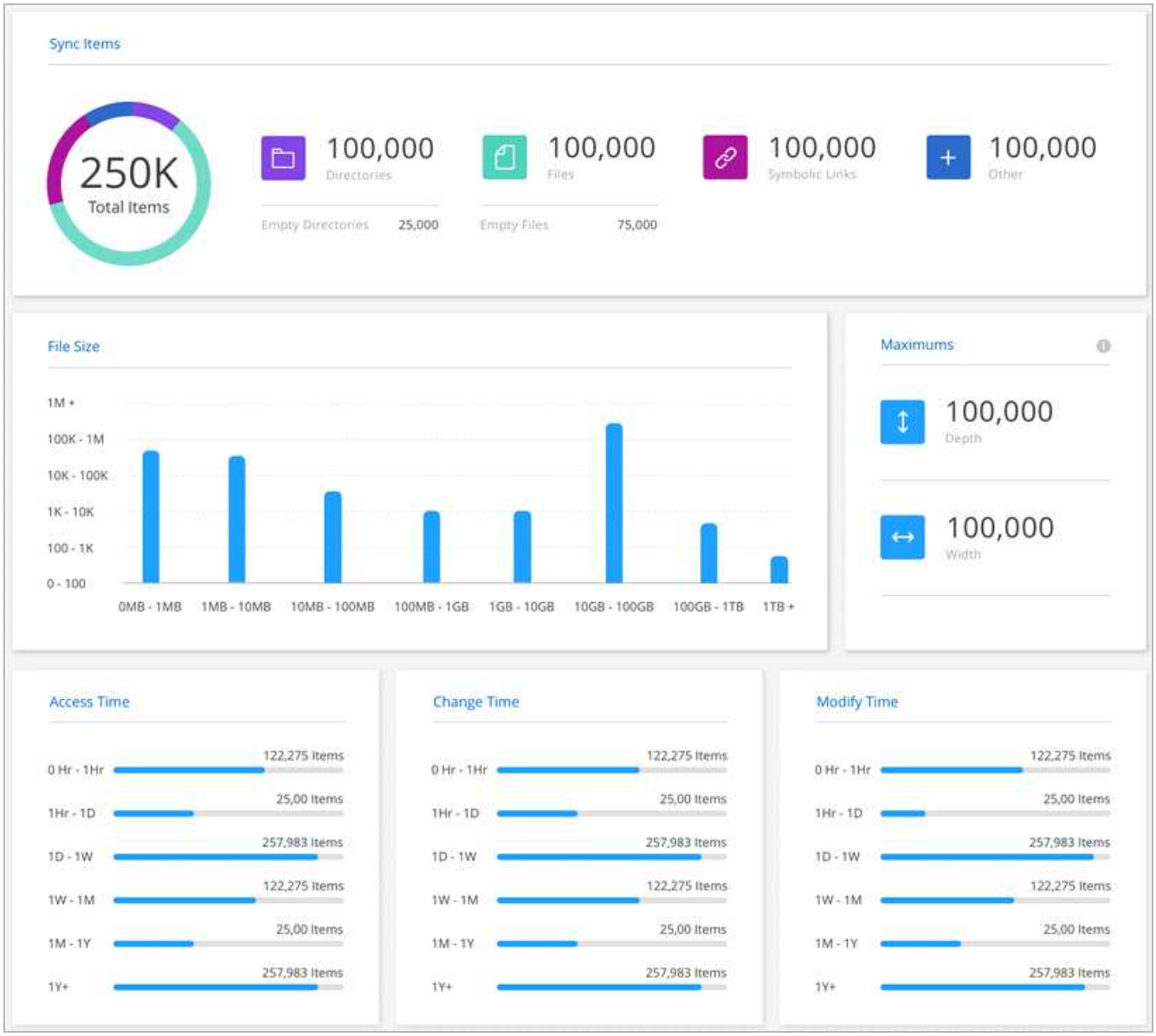
보고서를 생성할 때마다 복사 및 동기화가 경로를 스캔한 다음 세부 정보를 보고서로 컴파일합니다.

단계

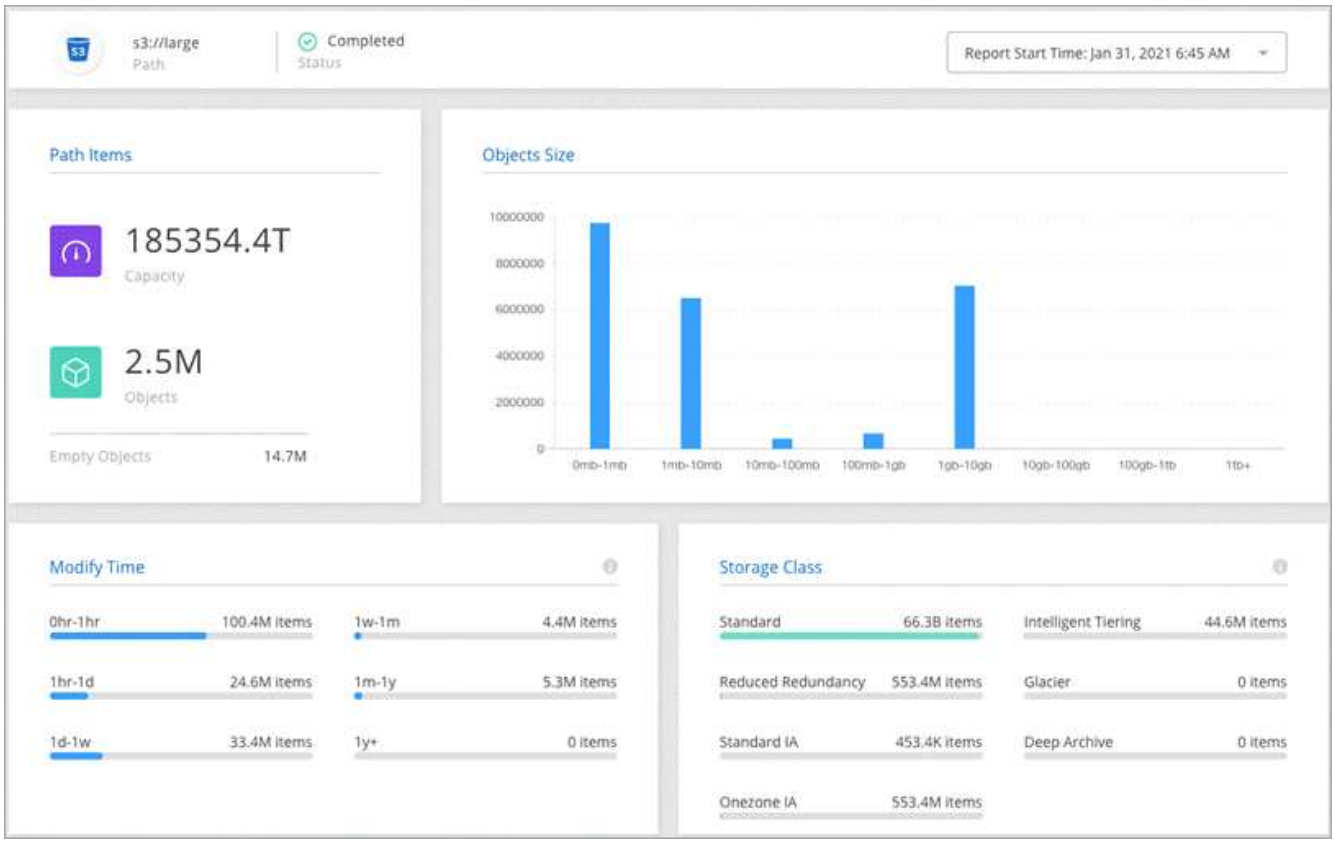
1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 보고서*를 선택합니다.

   각 동기화 관계의 경로(소스 또는 대상)가 표에 표시됩니다.
3. 보고서 작업 열에서 특정 경로로 이동하여 *만들기*를 선택하거나 작업 메뉴를 선택하고 *새로 만들기*를 선택합니다.
4. 보고서가 준비되면 작업 메뉴를 선택하고 *보기*를 선택하세요.

   다음은 파일 시스템 경로에 대한 보고서 샘플입니다.



다음은 개체 저장소에 대한 샘플 보고서입니다.

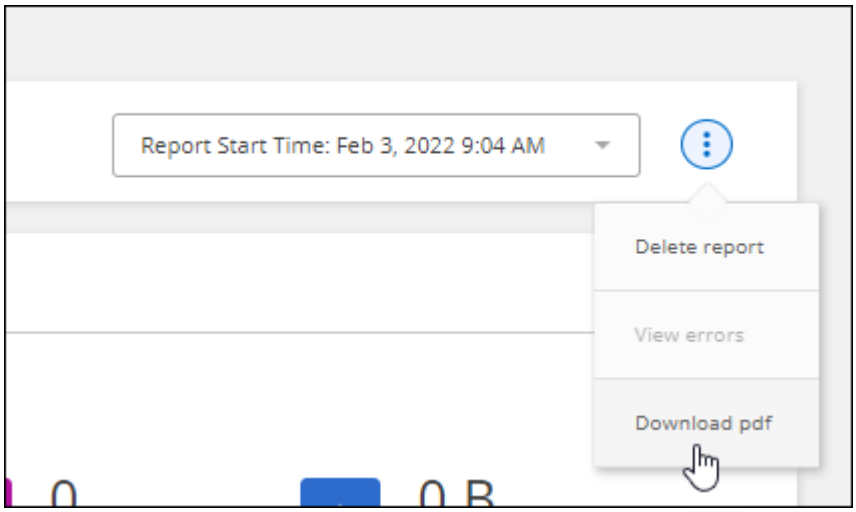


보고서 다운로드

오프라인에서 보거나 공유할 수 있도록 보고서를 PDF로 다운로드할 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 보고서*를 선택합니다.
3. 보고서 작업 열에서 작업 메뉴를 선택하고 *보기*를 선택합니다.
4. 보고서 오른쪽 상단에서 작업 메뉴를 선택하고 *pdf 다운로드*를 선택하세요.



보고서 오류 보기

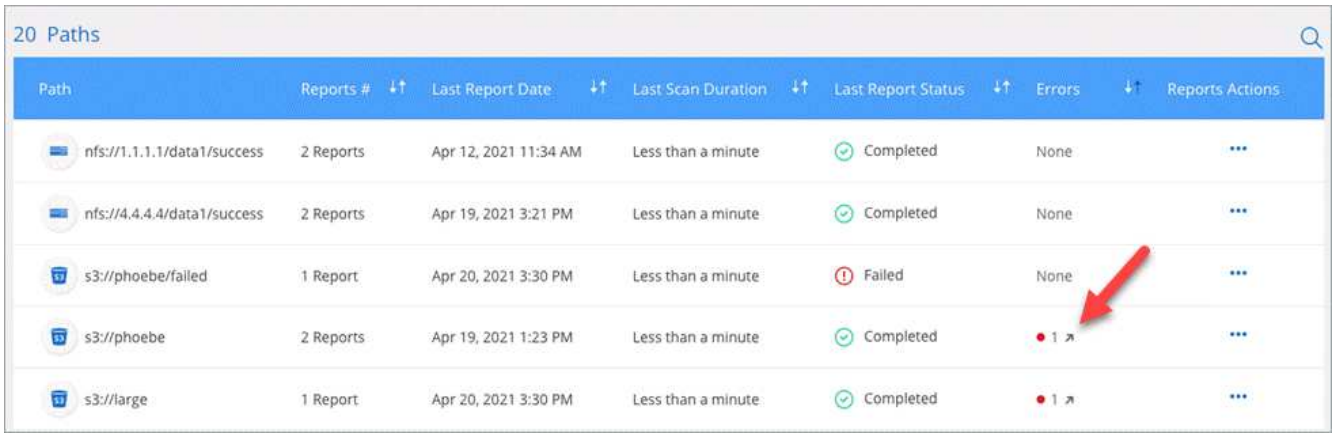
경로 테이블은 최신 보고서에 오류가 있는지 여부를 식별합니다. 오류는 Copy and Sync가 경로를 스캔할 때 발생한 문제를 나타냅니다.

예를 들어, 보고서에 권한 거부 오류가 포함될 수 있습니다. 이러한 유형의 오류는 Copy and Sync가 전체 파일과 디렉터리를 검색하는 기능에 영향을 미칠 수 있습니다.

오류 목록을 확인한 후 문제를 해결하고 보고서를 다시 실행할 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *동기화 > 보고서*를 선택합니다.
3. 오류 열에서 보고서에 오류가 있는지 확인합니다.
4. 오류가 있는 경우 오류 개수 옆에 있는 화살표를 선택하세요.



5. 오류에 있는 정보를 사용하여 문제를 해결하세요.

   문제를 해결한 후에는 다음에 보고서를 실행할 때 오류가 나타나지 않아야 합니다.

보고서 삭제

보고서에 수정한 오류가 포함되어 있거나, 보고서가 제거한 동기화 관계와 관련된 경우 해당 보고서를 삭제할 수 있습니다.

단계

1. *동기화 > 보고서*를 선택합니다.
2. 보고서 작업 열에서 경로에 대한 작업 메뉴를 선택하고 마지막 보고서 삭제 또는 *모든 보고서 삭제*를 선택합니다.
3. 보고서를 삭제할지 확인하세요.

NetApp Copy and Sync용 데이터 브로커 제거

필요한 경우 제거 스크립트를 실행하여 데이터 브로커와 NetApp Copy and Sync에 대해 데이터 브로커가 설치될 때 생성된 패키지 및 디렉터리를 제거합니다.

단계

1. 데이터 브로커 호스트에 로그인합니다.
2. 데이터 브로커 디렉토리로 변경: `/opt/netapp/databroker`
3. 다음 명령을 실행하세요.

```
chmod +x uninstaller-DataBroker.sh
./uninstaller-DataBroker.sh
```

4. 'y'를 눌러 제거를 확인하세요.

NetApp 복사 및 동기화 API

웹 UI를 통해 제공되는 NetApp 복사 및 동기화 기능은 RESTful API를 통해서도 사용할 수 있습니다.

시작하기

Copy and Sync API를 시작하려면 사용자 토큰과 NetApp 콘솔 계정 ID를 얻어야 합니다. API 호출을 할 때 Authorization 헤더에 토큰과 계정 ID를 추가해야 합니다.

단계

1. NetApp 콘솔에서 사용자 토큰을 얻습니다.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
                "username": "<user_email>",
                "scope": "profile",
                "audience": "https://api.cloud.netapp.com",
                "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
                "grant_type": "password",
                "password": "<user_password>"
}
```

클라이언트 ID가 없는 개인 이메일 계정을 사용하는 경우 기본 클라이언트 ID "QC3AgHk6qdbmC7Yyr82ApBwaaJLwRrNO"를 사용할 수 있습니다.

2. NetApp 콘솔 계정 ID를 얻으세요.

```
GET https://api.cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

이 API는 다음과 같은 응답을 반환합니다.

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. 각 API 호출의 Authorization 헤더에 사용자 토큰과 계정 ID를 추가합니다.

   예

   다음 예제에서는 Microsoft Azure에서 데이터 브로커를 만드는 API 호출을 보여줍니다. <user_token>과 <accountId>를 이전 단계에서 얻은 토큰과 ID로 바꾸기만 하면 됩니다.

```
POST https://api.cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

다음은 무엇인가요?

NetApp 콘솔의 사용자 토큰에는 만료 날짜가 있습니다. 토큰을 새로 고치려면 1단계의 API를 다시 호출해야 합니다.

API 응답에는 토큰이 만료되는 시점을 나타내는 "expires_in" 필드가 포함되어 있습니다.

목록 API 사용

목록 API는 비동기 API이므로 결과가 즉시 반환되지 않습니다(예: `GET /data-brokers/{id}/list-nfs-export-folders` 그리고 `GET /data-brokers/{id}/list-s3-buckets`). 서버에서 보내는 유일한 응답은 HTTP 상태 202입니다. 실제 결과를 얻으려면 다음을 사용해야 합니다. `GET /messages/client` API.

단계

1. 사용하려는 목록 API를 호출합니다.
2. 사용하다 `GET /messages/client` 작업 결과를 볼 수 있는 API입니다.
3. 방금 받은 ID를 추가하여 동일한 API를 사용하세요. `GET http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   ID는 호출할 때마다 변경됩니다. `GET /messages/client` API.

예

당신이 전화할 때 `list-s3-buckets` API, 결과가 즉시 반환되지 않습니다.

```
GET http://api.cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

결과는 HTTP 상태 코드 202입니다. 이는 메시지가 수락되었지만 아직 처리되지 않았음을 의미합니다.

작업 결과를 얻으려면 다음 API를 사용해야 합니다.

```
GET http://api.cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

결과는 ID 필드를 포함하는 하나의 객체가 있는 배열입니다. ID 필드는 서버가 보낸 마지막 메시지를 나타냅니다. 예를 들어:

```
[
    {
        "header": {
            "requestId": "init",
            "clientId": "init",
            "agentId": "init"
        },
        "payload": {
            "init": {}
        },
        "id": "5801"
    }
]
```

이제 방금 받은 ID를 사용하여 다음 API 호출을 수행합니다.

```
GET
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

그 결과, 일련의 메시지가 생성됩니다. 각 메시지 내부에는 작업 이름(키)과 결과(값)로 구성된 페이로드 객체가 있습니다. 예를 들어:

```
[
    {
        "payload": {
            "list-s3-buckets": [
                {
                    "tags": [
                        {
                            "Value": "100$",
                            "Key": "price"
                        }
                    ],
                    "region": {
                        "displayName": "US West (Oregon)",
                        "name": "us-west-2"
                    },
                    "name": "small"
                }
            ]
        },
        "header": {
            "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
            "clientId": "5beb032f548e6e35f4ed1ba9",
            "agentId": "5bed61f4489fb04e34a9aac6"
        },
        "id": "5802"
    }
]
```


API 참조

각 복사 및 동기화 API에 대한 설명서는 다음에서 제공됩니다. https://api.cloudsync.netapp.com/docs .

개념

NetApp Copy and Sync에 대한 라이선싱 개요

14일 무료 평가판이 종료된 후에는 NetApp 복사 및 동기화 관계에 대한 비용을 두 가지 방법으로 지불할 수 있습니다. 첫 번째 옵션은 AWS 또는 Azure에 가입하여 사용량에 따라 요금을 지불하거나 연간 요금을 지불하는 것입니다. 두 번째 옵션은 NetApp 에서 직접 라이선스를 구매하는 것입니다.

라이선스는 NetApp 콘솔이 아닌 NetApp Copy and Sync 또는 해당 웹사이트를 통해 관리해야 합니다.

마켓플레이스 구독

AWS 또는 Azure에서 Copy and Sync를 구독하면 시간당 요금이나 연간 요금을 지불할 수 있습니다. "AWS 또는 Azure를 통해 구독할 수 있습니다." , 청구를 원하는 곳에 따라 달라집니다.

시간당 구독

시간당 요금 지불 구독의 경우, 생성한 동기화 관계 수에 따라 시간당 요금이 청구됩니다.

- "Azure에서 가격 보기"
- "AWS에서 사용량에 따른 가격 책정 보기"

연간 구독

연간 구독은 선불로 지불하는 20개의 동기화 관계에 대한 라이선스를 제공합니다. 동기화 관계가 20개를 넘고 AWS를 통해 구독한 경우, 추가 관계에 대한 비용을 시간당으로 지불해야 합니다.

"AWS의 연간 가격 보기"

NetApp 의 라이센스

동기화 관계에 대한 비용을 미리 지불하는 또 다른 방법은 NetApp 에서 직접 라이선스를 구매하는 것입니다. 각 라이선스를 사용하면 최대 20개의 동기화 관계를 만들 수 있습니다.

이러한 라이선스는 AWS 또는 Azure 구독과 함께 사용할 수 있습니다. 예를 들어, 동기화 관계가 25개라면 라이선스를 사용하여 처음 20개 동기화 관계에 대한 요금을 지불한 다음, 나머지 5개 동기화 관계에 대해서는 AWS 또는 Azure에서 사용량에 따라 요금을 지불할 수 있습니다.

"라이센스를 구매하고 NetApp Copy and Sync에 추가하는 방법을 알아보세요." .

라이센스 조건

Copy and Sync에 BYOL(Bring Your Own License)을 구매한 고객은 라이선스 자격과 관련된 제한 사항을 알고 있어야 합니다.

- 고객은 배송일로부터 1년을 초과하지 않는 기간 동안 BYOL 라이선스를 활용할 권리가 있습니다.
- 고객은 BYOL 라이선스를 활용하여 소스와 대상 간에 총 20개의 개별 연결을 설정할 수 있으며, 이 연결은 최대

20개까지 허용됩니다(각각 "동기화 관계").

- 고객의 권한은 고객이 20개의 동기화 관계 제한에 도달했는지 여부와 관계없이 1년 라이선스 기간이 종료되면 만료됩니다.
- 고객이 라이선스를 갱신하기로 선택하는 경우, 이전 라이선스 부여와 관련된 사용되지 않은 동기화 관계는 라이선스 갱신으로 이월되지 않습니다.

NetApp Copy and Sync의 데이터 개인 정보 보호

NetApp NetApp Copy and Sync를 사용하는 동안 사용자가 제공하는 자격 증명에 액세스할 수 없습니다. 자격 증명은 네트워크에 있는 데이터 브로커 머신에 직접 저장됩니다.

선택한 구성에 따라 새 관계를 만들 때 복사 및 동기화에서 자격 증명을 입력하라는 메시지가 표시될 수 있습니다. 예를 들어, SMB 서버를 포함하는 관계를 설정하거나 AWS에 데이터 브로커를 배포하는 경우가 있습니다.

이러한 자격 증명은 항상 데이터 브로커 자체에 직접 저장됩니다. 데이터 브로커는 온프레미스든 클라우드 계정이든 네트워크의 머신에 상주합니다. 자격 증명은 NetApp 에 제공되지 않습니다.

자격 증명은 HashiCorp Vault를 사용하여 데이터 브로커 머신에서 로컬로 암호화됩니다.

NetApp 복사 및 동기화 기술 FAQ

이 FAQ는 질문에 대한 빠른 답변을 찾는 데 도움이 될 수 있습니다.

시작하기

다음 질문은 NetApp Copy and Sync를 시작하는 데 관한 것입니다.

NetApp Copy and Sync는 어떻게 작동하나요?

Copy and Sync는 NetApp 데이터 브로커 소프트웨어를 사용하여 소스에서 대상으로 데이터를 동기화합니다(이를 _동기화 관계_라고 합니다).

데이터 브로커 그룹은 소스와 대상 간의 동기화 관계를 제어합니다. 동기화 관계를 설정한 후 Copy and Sync는 소스 시스템을 분석하고 이를 여러 복제 스트림으로 분할하여 선택한 대상 데이터로 푸시합니다.

최초 복사 후, 복사 및 동기화는 사용자가 설정한 일정에 따라 변경된 데이터를 동기화합니다.

14일 무료 체험은 어떻게 진행되나요?

Copy and Sync에 가입하면 14일 무료 체험이 시작됩니다. 14일 동안 생성한 복사 및 동기화 관계에 대해서는 NetApp 요금이 부과되지 않습니다. 하지만 배포하는 모든 데이터 브로커에 대한 리소스 요금은 여전히 적용됩니다.

복사 및 동기화 비용은 얼마인가요?

Copy and Sync를 사용하는 데에는 서비스 요금과 리소스 요금이라는 두 가지 유형의 비용이 있습니다.

서비스 요금

사용량에 따른 가격 책정의 경우, 복사 및 동기화 서비스 요금은 귀하가 만든 동기화 관계 수에 따라 시간당으로

부과됩니다.

- "AWS에서 사용량에 따른 가격 책정 보기"
- "AWS의 연간 가격 보기"
- "Azure에서 가격 보기"

복사 및 동기화 라이선스는 NetApp 담당자를 통해서도 구매할 수 있습니다. 각 라이선스는 12개월 동안 20개의 동기화 관계를 지원합니다.

"라이센스에 대해 자세히 알아보세요" .

Azure NetApp Files 에서는 복사 및 동기화 관계가 무료입니다.

자원 요금

리소스 요금은 클라우드에서 데이터 브로커를 실행하는 데 드는 컴퓨팅 및 저장 비용과 관련됩니다.

Copy and Sync에 대한 요금은 어떻게 청구되며, 구독은 어떻게 관리하나요**?**

14일 무료 체험 기간이 종료된 후에는 두 가지 방법으로 동기화 관계에 대한 비용을 지불할 수 있습니다. 첫 번째 옵션은 AWS나 Azure에서 구독하는 것입니다. 이 경우 사용량에 따라 비용을 지불하거나 연간으로 지불할 수 있습니다. 두 번째 옵션은 NetApp 에서 직접 라이선스를 구매하는 것입니다. 어느 경우든 귀하의 구독은 Copy and Sync 사용자 인터페이스가 아닌 공급자 마켓플레이스를 통해 관리됩니다.

클라우드 외부에서 **Copy and Sync**를 사용할 수 있나요**?**

네, 클라우드가 아닌 아키텍처에서도 복사 및 동기화 기능을 사용할 수 있습니다. 소스와 타겟은 온프레미스에 있을 수 있으며 데이터 브로커 소프트웨어도 마찬가지입니다.

클라우드 외부에서 복사 및 동기화를 사용하는 것에 대한 주요 사항은 다음과 같습니다.

- 데이터 브로커 그룹은 Copy and Sync와 통신하기 위해 인터넷 연결이 필요합니다.
- NetApp 에서 직접 라이선스를 구매하지 않으면 PAYGO 복사 및 동기화 청구를 위해 AWS 또는 Azure 계정이 필요합니다.

복사 및 동기화 기능에 어떻게 접근하나요**?**

복사 및 동기화 기능은 NetApp 콘솔에서 사용할 수 있습니다. 콘솔 왼쪽 탐색에서 모바일 > *복사 및 동기화*를 선택합니다.

데이터 브로커 그룹이란 무엇인가요**?**

각 데이터 브로커는 데이터 브로커 그룹에 속합니다. 데이터 브로커를 그룹화하면 동기화 관계의 성능을 개선하는 데 도움이 됩니다.

지원되는 소스 및 대상

다음 질문은 동기화 관계에서 지원되는 소스 및 대상과 관련이 있습니다.

Copy and Sync는 어떤 소스와 대상을 지원합니까**?**

복사 및 동기화는 다양한 유형의 동기화 관계를 지원합니다. "전체 목록 보기" .

Copy and Sync는 어떤 버전의 **NFS**와 **SMB**를 지원합니까**?**

복사 및 동기화 기능은 NFS 버전 3 이상, SMB 버전 1 이상을 지원합니다.

"동기화 요구 사항에 대해 자세히 알아보세요" .

Amazon S3가 대상인 경우 데이터를 특정 **S3** 스토리지 클래스로 계층화할 수 있습니까**?**

네, AWS S3가 대상인 경우 특정 S3 스토리지 클래스를 선택할 수 있습니다.

- 표준(기본 클래스)
- 지능형 계층화
- 표준-빈번하지 않은 액세스
- 1존-접근 빈도 낮음
- 빙하 심층 기록 보관소
- Glacier Flexible Retrieval
- 빙하 즉시 검색

Azure Blob 스토리지의 스토리지 계층은 어떻게 되나요**?**

Blob 컨테이너가 대상인 경우 특정 Azure Blob 저장소 계층을 선택할 수 있습니다.

- 뜨거운 보관
- 시원한 보관

Google Cloud 스토리지 계층을 지원하시나요**?**

예, Google Cloud Storage 버킷이 대상인 경우 특정 스토리지 클래스를 선택할 수 있습니다.

- 기준
- 니어라인
- 콜드라인
- 보관소

네트워킹

다음 질문은 Copy and Sync에 대한 네트워킹 요구 사항과 관련이 있습니다.

Copy and Sync에 필요한 네트워킹 요구 사항은 무엇입니까**?**

복사 및 동기화 환경에서는 데이터 브로커 그룹이 선택한 프로토콜이나 개체 스토리지 API(Amazon S3, Azure Blob, IBM Cloud Object Storage)를 통해 소스 및 대상에 연결되어 있어야 합니다.

또한, 데이터 브로커 그룹은 Copy and Sync와 통신하고 몇몇 다른 서비스와 저장소에 접속할 수 있도록 포트 443을 통한 아웃바운드 인터넷 연결이 필요합니다.

자세한 내용은"네트워킹 요구 사항 검토" .

데이터 브로커와 함께 프록시 서버를 사용할 수 있나요?

네.

Copy and Sync는 기본 인증 여부와 관계없이 프록시 서버를 지원합니다. 데이터 브로커를 배포할 때 프록시 서버를 지정하는 경우 데이터 브로커의 모든 HTTP 및 HTTPS 트래픽은 프록시를 통해 라우팅됩니다. NFS나 SMB와 같은 HTTP가 아닌 트래픽은 프록시 서버를 통해 라우팅될 수 없습니다.

유일한 프록시 서버 제한 사항은 NFS 또는 Azure NetApp Files 동기화 관계에서 전송 중 데이터 암호화를 사용할 때입니다. 암호화된 데이터는 HTTPS를 통해 전송되며 프록시 서버를 통해 라우팅할 수 없습니다.

데이터 동기화

다음 질문은 데이터 동기화가 작동하는 방식과 관련이 있습니다.

동기화는 얼마나 자주 발생합니까?

기본 일정은 매일 동기화로 설정되어 있습니다. 초기 동기화 후에는 다음을 수행할 수 있습니다.

- 원하는 일수, 시간 또는 분으로 동기화 일정을 수정하세요.
- 동기화 일정 비활성화
- 동기화 일정을 삭제합니다(데이터는 손실되지 않으며 동기화 관계만 제거됩니다)

최소 동기화 일정은 무엇입니까?

최대 1분마다 데이터를 동기화하도록 관계를 예약할 수 있습니다.

파일 동기화에 실패하면 데이터 브로커 그룹이 다시 시도합니까? 아니면 시간이 초과되나요?

데이터 브로커 그룹은 단일 파일 전송에 실패해도 시간 초과가 발생하지 않습니다. 대신 데이터 브로커 그룹은 파일을 건너뛰기 전에 3번 다시 시도합니다. 재시도 값은 동기화 관계 설정에서 구성할 수 있습니다.

"동기화 관계의 설정을 변경하는 방법을 알아보세요" .

데이터 세트가 매우 큰 경우에는 어떻게 해야 하나요?

단일 디렉토리에 600,000개 이상의 파일이 포함되어 있는 경우"문의하기" 이를 통해 데이터 브로커 그룹이 페이로드를 처리하도록 구성하는 데 도움을 드릴 수 있습니다. 데이터 브로커 그룹에 추가 메모리를 추가해야 할 수도 있습니다.

마운트 지점에 있는 파일의 총 개수에는 제한이 없습니다. 60만 개 이상의 파일이 있는 대규모 디렉토리의 경우 계층 구조(최상위 디렉토리 또는 하위 디렉토리)에 관계없이 추가 메모리가 필요합니다.

보안

다음은 보안과 관련된 질문입니다.

복사 및 동기화는 안전한가요?

네. 모든 복사 및 동기화 네트워킹 연결은 다음을 사용하여 수행됩니다. "Amazon Simple Queue Service(SQS)" .

데이터 브로커 그룹과 Amazon S3, Azure Blob, Google Cloud Storage, IBM Cloud Object Storage 간의 모든 통신은 HTTPS 프로토콜을 통해 이루어집니다.

온프레미스(소스 또는 대상) 시스템에서 복사 및 동기화를 사용하는 경우 권장하는 몇 가지 연결 옵션은 다음과 같습니다.

- 인터넷 라우팅이 아닌 AWS Direct Connect, Azure ExpressRoute 또는 Google Cloud Interconnect 연결(지정한 클라우드 네트워크와만 통신 가능)
- 온프레미스 게이트웨이 장치와 클라우드 네트워크 간의 VPN 연결
- S3 버킷, Azure Blob 스토리지 또는 Google Cloud Storage를 사용하여 더욱 안전하게 데이터를 전송하려면 Amazon Private S3 Endpoint, Azure Virtual Network 서비스 엔드포인트 또는 Private Google Access를 설정할 수 있습니다.

이러한 방법을 사용하면 온프레미스 NAS 서버와 Copy and Sync 데이터 브로커 그룹 간에 보안 연결이 설정됩니다.

Copy and Sync를 사용하면 데이터가 암호화되나요?

- 복사 및 동기화는 소스 및 대상 NFS 서버 간의 전송 중 데이터 암호화를 지원합니다. "자세히 알아보기" .
- SMB의 경우, 복사 및 동기화는 서버 측에서 암호화한 SMB 3.0 및 3.11 데이터를 지원합니다. 복사 및 동기화는 암호화된 데이터를 소스에서 대상으로 복사하고, 대상에서는 데이터가 암호화된 상태로 유지됩니다.

  복사 및 동기화는 SMB 데이터 자체를 암호화할 수 없습니다.

- Amazon S3 버킷이 동기화 관계의 대상인 경우 AWS KMS 암호화 또는 AES-256 암호화를 사용하여 데이터 암호화를 활성화할지 선택할 수 있습니다.
- Google Storage 버킷이 동기화 관계의 대상인 경우 기본 Google 관리 암호화 키를 사용할지, 아니면 사용자 고유의 KMS 키를 사용할지 선택할 수 있습니다.

권한

다음 질문은 데이터 권한과 관련이 있습니다.

SMB 데이터 권한이 대상 위치와 동기화되어 있습니까?

소스 SMB 공유와 대상 SMB 공유 간, 그리고 소스 SMB 공유에서 개체 스토리지(ONTAP S3 제외)로의 액세스 제어 목록(ACL)을 보존하도록 복사 및 동기화를 설정할 수 있습니다.

> 복사 및 동기화는 개체 스토리지에서 SMB 공유로 ACL을 복사하는 것을 지원하지 않습니다.

"SMB 공유 간에 ACL을 복사하는 방법을 알아보세요" .

NFS 데이터 권한이 대상 위치와 동기화됩니까?

복사 및 동기화는 다음과 같이 NFS 서버 간에 NFS 권한을 자동으로 복사합니다.

- NFS 버전 3: 복사 및 동기화는 권한과 사용자 그룹 소유자를 복사합니다.

- NFS 버전 4: 복사 및 동기화는 ACL을 복사합니다.

개체 스토리지 메타데이터

어떤 종류의 동기화 관계가 개체 저장소 메타데이터를 보존합니까**?**

복사 및 동기화는 다음 유형의 동기화 관계에 대해 소스에서 대상으로 개체 스토리지 메타데이터를 복사합니다.

- 아마존 S3 → 아마존 S3 [1]
- 아마존 S3 → StorageGRID
- StorageGRID → 아마존 S3
- StorageGRID → StorageGRID
- StorageGRID → Google 클라우드 스토리지
- Google 클라우드 스토리지 → StorageGRID [1]
- Google Cloud Storage → IBM Cloud Object Storage [1]
- 구글 클라우드 스토리지 → 아마존 S3 [1]
- Amazon S3 → Google 클라우드 스토리지
- IBM Cloud Object Storage → Google Cloud Storage
- StorageGRID → IBM 클라우드 객체 스토리지
- IBM 클라우드 객체 스토리지 → StorageGRID
- IBM 클라우드 객체 스토리지 → IBM 클라우드 객체 스토리지

[1] 이러한 동기화 관계에는 다음이 필요합니다."동기화 관계를 생성할 때 개체 복사 설정을 활성화합니다." .

NFS 또는 **SMB**가 소스인 동기화 중에 어떤 종류의 메타데이터가 복제됩니까**?**

사용자 ID, 수정 시간, 액세스 시간, GID와 같은 메타데이터는 기본적으로 복제됩니다. 사용자는 동기화 관계를 생성할 때 필수로 표시하여 CIF에서 ACL 복제를 선택할 수 있습니다.

성능

다음 질문은 복사 및 동기화 성능과 관련이 있습니다.

동기화 관계의 진행률 표시기는 무엇을 나타냅니까**?**

동기화 관계는 데이터 브로커 그룹의 네트워크 어댑터의 처리량을 보여줍니다. 여러 데이터 브로커를 사용하여 동기화 성능을 가속화하는 경우 처리량은 모든 트래픽의 합계가 됩니다. 이 처리량은 20초마다 새로 고쳐집니다.

성능 문제가 발생하고 있습니다**.** 동시 전송 수를 제한할 수 있나요**?**

매우 큰 파일(각각 여러 TiB)이 있는 경우 전송 프로세스를 완료하는 데 시간이 오래 걸릴 수 있으며 성능에 영향을 줄 수 있습니다.

동시 전송 수를 제한하면 도움이 될 수 있습니다. "도움이 필요하면 저희에게 연락하세요" .

Azure NetApp Files 에서 성능이 저하되는 이유는 무엇입니까**?**

디스크 서비스 수준이 표준인 경우 Azure NetApp Files 에서 데이터를 동기화할 때 오류 및 성능 문제가 발생할 수 있습니다.

동기화 성능을 향상시키려면 서비스 수준을 프리미엄 또는 울트라로 변경하세요.

"Azure NetApp Files 서비스 수준 및 처리량에 대해 자세히 알아보세요." .

그룹에는 몇 명의 데이터 브로커가 필요합니까**?**

새로운 관계를 만들 때는 그룹 내 단일 데이터 브로커로 시작합니다(가속 동기화 관계에 속한 기존 데이터 브로커를 선택한 경우는 제외). 많은 경우, 단일 데이터 브로커가 동기화 관계에 대한 성능 요구 사항을 충족할 수 있습니다. 그렇지 않은 경우 그룹에 추가 데이터 브로커를 추가하여 동기화 성능을 가속화할 수 있습니다. 하지만 먼저 동기화 성능에 영향을 줄 수 있는 다른 요소를 확인해야 합니다.

여러 요소가 데이터 전송 성능에 영향을 미칠 수 있습니다. 네트워크 대역폭, 지연 시간, 네트워크 토폴로지는 물론, 데이터 브로커 VM 사양과 스토리지 시스템 성능으로 인해 전반적인 동기화 성능에 영향을 받을 수 있습니다. 예를 들어, 그룹 내 단일 데이터 브로커는 최대 100MB/s에 도달할 수 있는 반면, 대상의 디스크 처리량은 최대 64MB/s만 허용할 수 있습니다. 결과적으로 데이터 브로커 그룹은 계속해서 데이터를 복사하려고 시도하지만 대상은 데이터 브로커 그룹의 성능을 충족할 수 없습니다.

따라서 대상의 네트워킹 성능과 디스크 처리량을 꼭 확인하세요.

그런 다음 그룹에 추가 데이터 브로커를 추가하여 해당 관계의 부하를 공유함으로써 동기화 성능을 가속화하는 것을 고려할 수 있습니다. "동기화 성능을 가속화하는 방법을 알아보세요" .

삭제하기

다음 질문은 소스와 대상에서 동기화 관계와 데이터를 삭제하는 것과 관련이 있습니다.

복사 및 동기화 관계를 삭제하면 어떻게 되나요**?**

관계를 삭제하면 향후 모든 데이터 동기화가 중단되고 결제가 종료됩니다. 대상과 동기화된 모든 데이터는 그대로 유지됩니다.

소스 서버에서 무언가를 삭제하면 어떻게 되나요**?** 타겟에서도 제거되나요**?**

기본적으로 활성 동기화 관계가 있는 경우 소스 서버에서 삭제된 항목은 다음 동기화 중에 대상 서버에서 삭제되지 않습니다. 하지만 각 관계에 대한 동기화 설정에는 소스에서 파일이 삭제된 경우 복사 및 동기화를 통해 대상 위치에서도 파일이 삭제되도록 정의할 수 있는 옵션이 있습니다.

"동기화 관계의 설정을 변경하는 방법을 알아보세요" .

타겟에서 무언가를 삭제하면 어떻게 되나요**?** 내 소스에서도 제거되나요**?**

대상에서 항목을 삭제해도 소스에서는 삭제되지 않습니다. 관계는 일방적, 즉 출처에서 대상으로 향하는 관계입니다. 다음 동기화 주기에서 복사 및 동기화는 소스와 대상을 비교하여 항목이 누락되었음을 확인하고, 복사 및 동기화는 해당 항목을 소스에서 대상으로 다시 복사합니다.

문제 해결

"NetApp 지식 기반: 복사 및 동기화 FAQ: 지원 및 문제 해결"

데이터 브로커 심층 분석

다음 질문은 데이터 브로커와 관련이 있습니다.

데이터 브로커의 아키텍처를 설명해 주시겠습니까?

확신하는. 가장 중요한 사항은 다음과 같습니다.

- 데이터 브로커는 Linux 호스트에서 실행되는 node.js 애플리케이션입니다.
- Copy and Sync는 다음과 같이 데이터 브로커를 배포합니다.
  - AWS: AWS CloudFormation 템플릿에서
  - Azure: Azure Resource Manager에서
  - Google: Google Cloud Deployment Manager에서
  - 자신의 Linux 호스트를 사용하는 경우 소프트웨어를 수동으로 설치해야 합니다.
- 데이터 브로커 소프트웨어는 자동으로 최신 버전으로 업그레이드됩니다.
- 데이터 브로커는 AWS SQS를 안정적이고 안전한 통신 채널로 사용하고 제어 및 모니터링을 위해 사용합니다. SQS는 또한 지속성 계층을 제공합니다.
- 그룹에 추가 데이터 브로커를 추가하여 전송 속도를 높이고 가용성을 높일 수 있습니다. 하나의 데이터 브로커에 장애가 발생하더라도 서비스 회복성이 있습니다.

지식과 지원

지원 등록

BlueXP 와 해당 스토리지 솔루션 및 서비스에 대한 기술 지원을 받으려면 지원 등록이 필요합니다. Cloud Volumes ONTAP 시스템의 주요 워크플로를 활성화하려면 지원 등록도 필요합니다.

지원에 등록해도 클라우드 공급자 파일 서비스에 대한 NetApp 지원은 제공되지 않습니다. 클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 BlueXP 설명서에서 "도움말 받기"를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

지원 등록 개요

지원 자격을 활성화하기 위한 등록 방법은 두 가지가 있습니다.

- BlueXP 계정 일련 번호를 등록합니다(BlueXP 의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호).

  이는 BlueXP 내의 모든 서비스에 대한 단일 지원 구독 ID 역할을 합니다. 각 BlueXP 계정 수준 지원 구독을 등록해야 합니다.

- 클라우드 공급업체의 마켓플레이스에서 구독과 관련된 Cloud Volumes ONTAP 일련 번호를 등록합니다(20자리 909201xxxxxxxx 일련 번호).

  이러한 일련 번호는 일반적으로 _PAYGO 일련 번호_라고 하며 Cloud Volumes ONTAP 배포 시 BlueXP 에서 생성됩니다.

두 가지 유형의 일련 번호를 모두 등록하면 지원 티켓 개설 및 자동 사례 생성과 같은 기능을 사용할 수 있습니다. 아래 설명된 대로 BlueXP 에 NetApp 지원 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

NetApp 지원을 위해 **BlueXP** 등록

지원을 등록하고 지원 자격을 활성화하려면 BlueXP 조직(또는 계정)의 한 사용자가 NetApp 지원 사이트 계정을 BlueXP 로그인과 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp 지원 사이트(NSS) 계정이 있는지 여부에 따라 달라집니다.

NSS 계정이 있는 기존 고객

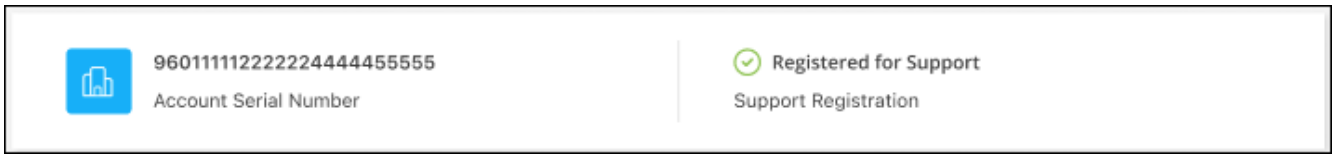
NSS 계정이 있는 NetApp 고객이라면 BlueXP 통해 지원을 받기 위해 등록하기만 하면 됩니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 *자격 증명*을 선택합니다.
2. *사용자 자격 증명*을 선택하세요.

3. *NSS 자격 증명 추가*를 선택하고 NetApp 지원 사이트(NSS) 인증 프롬프트를 따릅니다.
4. 등록 과정이 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택하고 *지원*을 선택하세요.

   리소스 페이지에는 귀하의 BlueXP 조직이 지원을 위해 등록되어 있다는 것이 표시되어야 합니다.



   다른 BlueXP 사용자는 NetApp 지원 사이트 계정을 BlueXP 로그인과 연결하지 않은 경우 이와 동일한 지원 등록 상태를 볼 수 없습니다. 하지만 그렇다고 해서 BlueXP 조직이 지원에 등록되지 않았다는 의미는 아닙니다. 조직 내 한 명의 사용자가 이러한 단계를 따랐다면 귀하의 조직은 등록된 것입니다.

기존 고객이지만 **NSS** 계정이 없습니다**.**

기존 라이선스와 일련 번호는 있지만 NSS 계정이 없는 기존 NetApp 고객인 경우 NSS 계정을 만들고 BlueXP 로그인과 연결해야 합니다.

단계

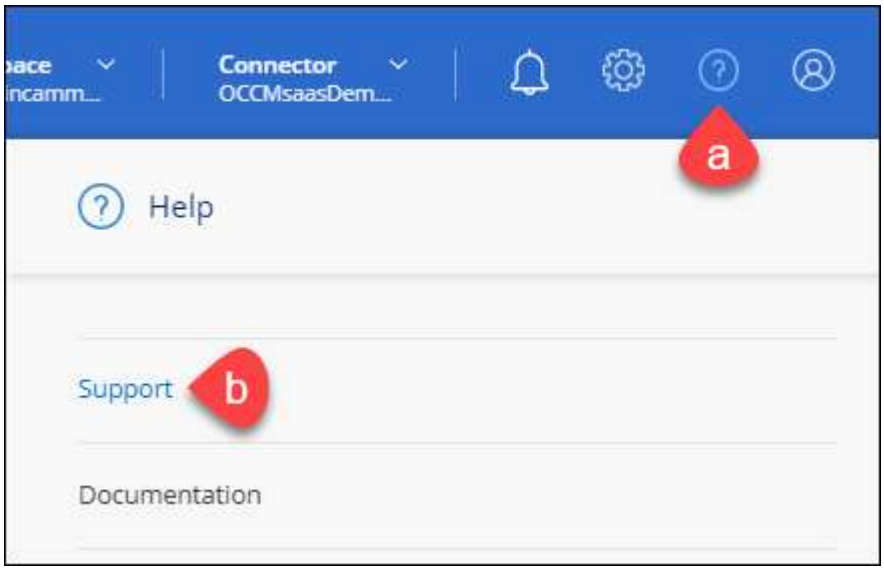
1. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
   b. 위에 사용된 BlueXP 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 계정 처리가 빨라집니다.
2. 다음 단계를 완료하여 새 NSS 계정을 BlueXP 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

NetApp 의 새로운 기능

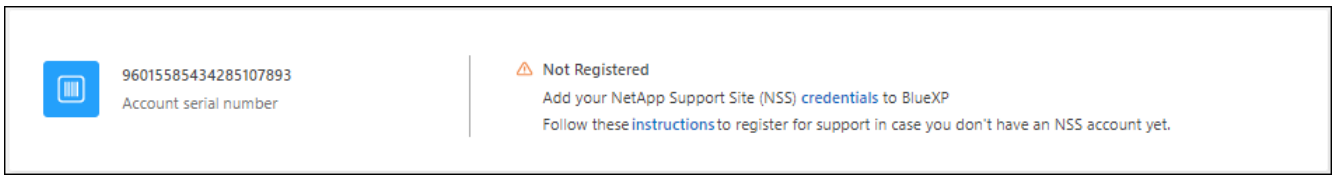
NetApp 처음 사용하시고 NSS 계정이 없으신 경우 아래의 각 단계를 따르세요.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.



2. 지원 등록 페이지에서 계정 ID 일련 번호를 찾으세요.



3. 로 이동 "NetApp 지원 등록 사이트" *저는 등록된 NetApp 고객이 아닙니다*를 선택하세요.
4. 필수 입력란(빨간색 별표가 있는 항목)을 작성해 주세요.
5. 제품군 필드에서 *클라우드 관리자*를 선택한 다음 해당 청구 제공자를 선택하세요.
6. 위의 2단계에서 계정 일련번호를 복사하고 보안 검사를 완료한 다음 NetApp의 글로벌 데이터 개인정보 보호정책을 읽었는지 확인하세요.

   이 안전한 거래를 마무리하기 위해 제공된 사서함으로 이메일이 즉시 전송됩니다. 몇 분 안에 인증 이메일이 도착하지 않으면 스팸 폴더를 확인하세요.

7. 이메일 내에서 작업을 확인하세요.

   확인을 클릭하면 귀하의 요청이 NetApp 에 제출되고 NetApp 지원 사이트 계정을 만드는 것이 좋습니다.

8. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
   b. 위에 사용된 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 처리 속도가 빨라집니다.

당신이 완료한 후

이 과정에서 NetApp 귀하에게 연락을 드릴 것입니다. 이는 신규 사용자를 대상으로 한 일회성 온보딩 과정입니다.

NetApp 지원 사이트 계정이 있으면 아래 단계를 완료하여 계정을 BlueXP 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

Cloud Volumes ONTAP 지원을 위한 NSS 자격 증명 연결

Cloud Volumes ONTAP 에 대한 다음과 같은 주요 워크플로를 활성화하려면 NetApp 지원 사이트 자격 증명을 BlueXP 조직과 연결해야 합니다.

- 지원을 위해 Pay-as-you-go Cloud Volumes ONTAP 시스템 등록

  시스템 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스하려면 NSS 계정을 제공해야 합니다.

- BYOL(Bring Your Own License)을 사용할 때 Cloud Volumes ONTAP 배포

  BlueXP 귀하의 라이선스 키를 업로드하고 귀하가 구매한 기간 동안 구독을 활성화하려면 귀하의 NSS 계정을 제공하는 것이 필요합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리스로 업그레이드

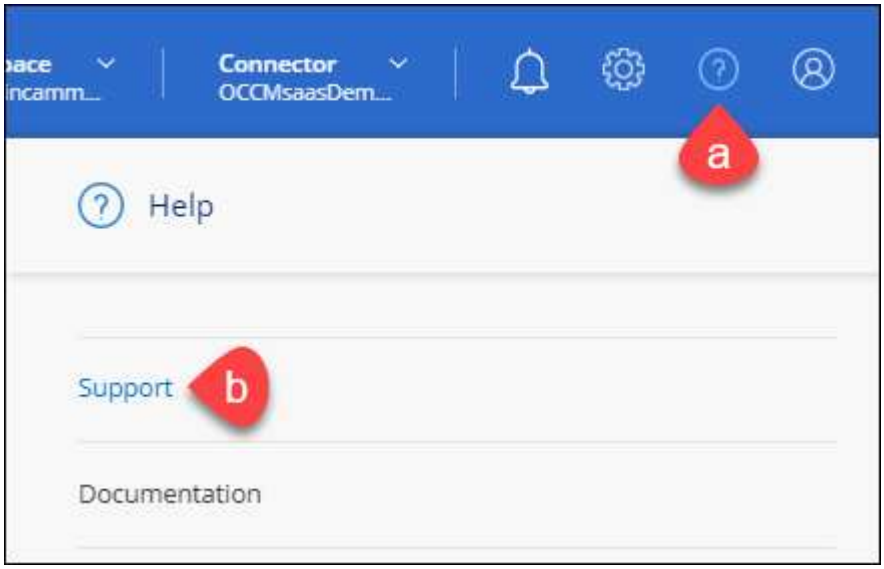
NSS 자격 증명을 BlueXP 조직에 연결하는 것은 BlueXP 사용자 로그인에 연결된 NSS 계정과 다릅니다.

이러한 NSS 자격 증명은 특정 BlueXP 조직 ID와 연결됩니다. BlueXP 조직에 속한 사용자는 *지원 > NSS 관리*에서 이러한 자격 증명에 액세스할 수 있습니다.

- 고객 수준 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있습니다.
- 파트너 또는 리셀러 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.



2. *NSS 관리 > NSS 계정 추가*를 선택하세요.
3. 메시지가 표시되면 *계속*을 선택하여 Microsoft 로그인 페이지로 리디렉션됩니다.

   NetApp 지원 및 라이선싱에 특화된 인증 서비스를 위한 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 NetApp 지원 사이트에 등록된 이메일 주소와 비밀번호를 입력하여 인증 과정을 진행합니다.

   이러한 작업을 통해 BlueXP 라이선스 다운로드, 소프트웨어 업그레이드 확인, 향후 지원 등록과 같은 작업에 NSS 계정을 사용할 수 있습니다.

   다음 사항에 유의하세요.

   - NSS 계정은 고객 수준 계정이어야 합니다(게스트나 임시 계정이어서는 안 됩니다). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
   - 해당 계정이 파트너 수준 계정인 경우 NSS 계정은 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하는데 파트너 수준 계정이 이미 있는 경우 다음과 같은 오류 메시지가 표시됩니다.

     "이 계정에는 다른 유형의 NSS 사용자가 이미 있으므로 NSS 고객 유형이 허용되지 않습니다."

   기존 고객 수준 NSS 계정이 있고 파트너 수준 계정을 추가하려는 경우에도 마찬가지입니다.

   - 로그인에 성공하면 NetApp NSS 사용자 이름을 저장합니다.

     이는 귀하의 이메일에 매핑되는 시스템 생성 ID입니다. **NSS** 관리 페이지에서 이메일을 표시할 수 있습니다. •••

메뉴.

- 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 자격 증명 업데이트 옵션도 있습니다. ••• 메뉴.

  이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이 계정의 토큰은 90일 후에 만료됩니다. 이에 대한 알림이 게시됩니다.

도움을 받으세요

NetApp BlueXP 와 클라우드 서비스에 대한 다양한 지원을 제공합니다. 지식 베이스(KB) 문서 및 커뮤니티 포럼 등 다양한 무료 셀프 지원 옵션을 연중무휴 24시간 이용하실 수 있습니다. 지원 등록 시 웹 티켓팅을 통한 원격 기술 지원이 제공됩니다.

클라우드 공급자 파일 서비스에 대한 지원을 받으세요

클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 BlueXP 설명서에서 "도움말 받기"를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

BlueXP 와 해당 스토리지 솔루션 및 서비스에 대한 구체적인 기술 지원을 받으려면 아래에 설명된 지원 옵션을 이용하세요.

셀프 지원 옵션 사용

다음 옵션은 주 7일, 하루 24시간 무료로 이용 가능합니다.

- 설명서

  현재 보고 있는 BlueXP 문서입니다.

- "지식 기반"

  BlueXP 지식 기반을 검색하여 문제 해결에 도움이 되는 문서를 찾아보세요.

- "커뮤니티"

  현재 진행 중인 토론을 팔로우하거나 새로운 토론을 만들려면 BlueXP 커뮤니티에 가입하세요.

NetApp 지원을 통해 사례 만들기

위에 나열된 셀프 지원 옵션 외에도, 지원을 활성화한 후 NetApp 지원 전문가와 협력하여 문제를 해결할 수 있습니다.

시작하기 전에

- 사례 만들기 기능을 사용하려면 먼저 NetApp 지원 사이트 자격 증명을 BlueXP 로그인과 연결해야 합니다. "BlueXP 로그인과 관련된 자격 증명을 관리하는 방법을 알아보세요." .

- 일련 번호가 있는 ONTAP 시스템에 대한 사례를 개설하는 경우 NSS 계정은 해당 시스템의 일련 번호와 연결되어야 합니다.

단계

1. BlueXP 에서 *도움말 > 지원*을 선택하세요.
2. 리소스 페이지에서 기술 지원 아래에 있는 사용 가능한 옵션 중 하나를 선택하세요.

   a. 전화로 상담원과 통화하고 싶으시면 *전화하기*를 선택하세요. netapp.com에서 전화할 수 있는 전화번호가 나열된 페이지로 이동하게 됩니다.

   b. NetApp 지원 전문가에게 티켓을 열려면 *사례 만들기*를 선택하세요.

      - 서비스: 문제와 관련된 서비스를 선택하세요. 예를 들어, BlueXP 서비스 내 워크플로나 기능에 대한 기술 지원 문제에 특화되어 있습니다.
      - 작업 환경: 스토리지에 해당되는 경우 * Cloud Volumes ONTAP* 또는 *온프레미스*를 선택한 다음 연관된 작업 환경을 선택합니다.

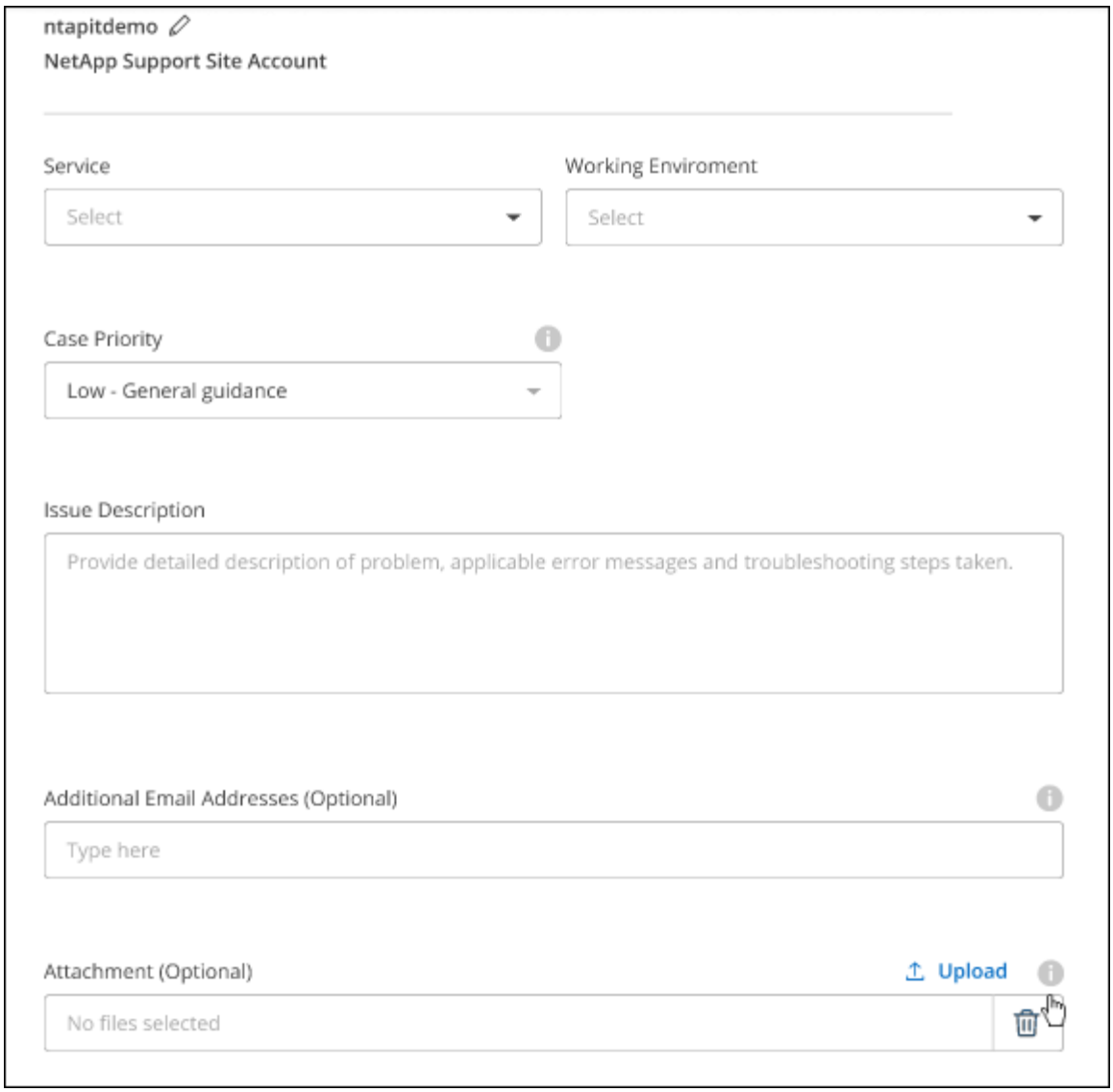
        작업 환경 목록은 서비스의 상단 배너에서 선택한 BlueXP 조직(또는 계정), 프로젝트(또는 작업 공간) 및 커넥터의 범위 내에 있습니다.

      - 사례 우선순위: 낮음, 보통, 높음 또는 중요로 사례의 우선순위를 선택합니다.

        이러한 우선순위에 대한 자세한 내용을 알아보려면 필드 이름 옆에 있는 정보 아이콘 위에 마우스를 올려놓으세요.

      - 문제 설명: 해당 오류 메시지나 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공하세요.
      - 추가 이메일 주소: 이 문제를 다른 사람에게 알리려면 추가 이메일 주소를 입력하세요.
      - 첨부파일(선택사항): 최대 5개의 첨부파일을 한 번에 하나씩 업로드하세요.

        첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.



당신이 완료한 후

지원 사례 번호가 포함된 팝업이 나타납니다. NetApp 지원 전문가가 귀하의 사례를 검토하고 곧 연락드릴 것입니다.

지원 사례 기록을 보려면 *설정 > 타임라인*을 선택하고 "지원 사례 만들기"라는 이름의 작업을 찾으세요. 가장 오른쪽에 있는 버튼을 누르면 동작을 확장하여 자세한 내용을 볼 수 있습니다.

사례를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대해 사례를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 해당 계정과 연결된 기록상 회사가 BlueXP 계정 일련 번호에 대한 기록상 회사와 동일하지 않다는 것을 의미할 수 있습니다(예: 960xxxx) 또는 작업 환경 일련 번호. 다음 옵션 중 하나를 사용하여 도움을 요청할 수 있습니다.

- 제품 내 채팅을 사용하세요
- 비기술적 사례를 제출하세요 https://mysupport.netapp.com/site/help

지원 사례 관리(미리 보기)

BlueXP 에서 직접 활성화된 지원 사례와 해결된 지원 사례를 보고 관리할 수 있습니다. 귀하의 NSS 계정 및 회사와 관련된 사례를 관리할 수 있습니다.

사례 관리 기능은 미리 보기로 제공됩니다. 우리는 이 경험을 더욱 개선하고 향후 릴리스에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 이용해 피드백을 보내주세요.

다음 사항에 유의하세요.

- 페이지 상단의 사례 관리 대시보드는 두 가지 보기를 제공합니다.
  - 왼쪽 보기는 귀하가 제공한 NSS 계정 사용자에 의해 지난 3개월 동안 열린 총 사례를 보여줍니다.
  - 오른쪽 보기는 사용자 NSS 계정을 기준으로 지난 3개월 동안 회사 수준에서 열린 총 사례를 보여줍니다.

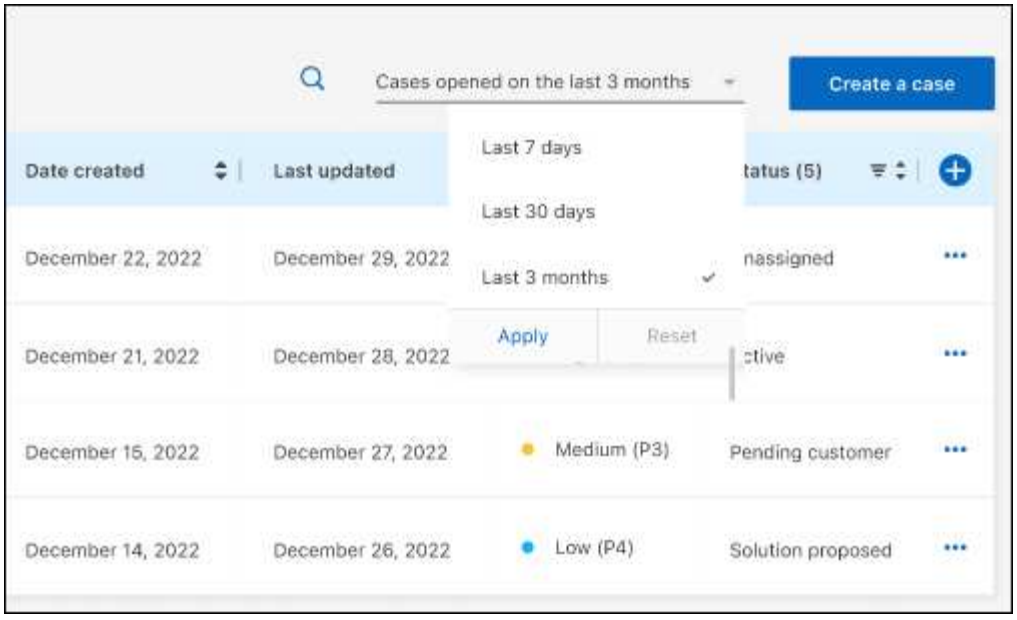
  표의 결과는 귀하가 선택한 보기와 관련된 사례를 반영합니다.
- 관심 있는 열을 추가하거나 제거할 수 있으며, 우선순위 및 상태와 같은 열의 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

  자세한 내용은 아래 단계를 참조하세요.
- 사례별로 사례 메모를 업데이트하거나 아직 닫힘 또는 닫힘 보류 상태가 아닌 사례를 닫는 기능을 제공합니다.

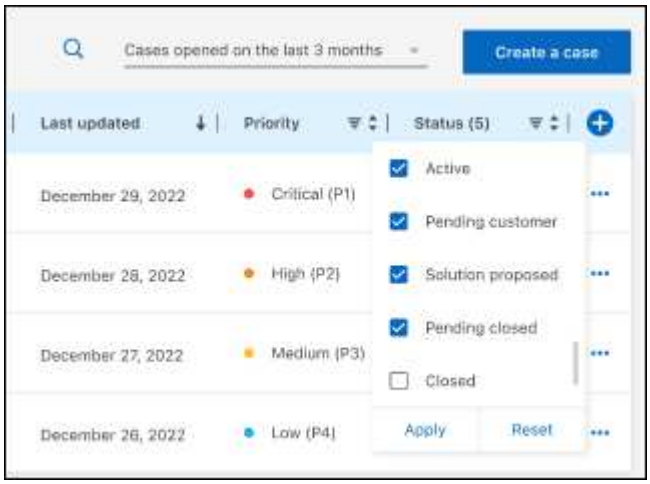
단계

1. BlueXP 에서 *도움말 > 지원*을 선택하세요.
2. *사례 관리*를 선택하고 메시지가 표시되면 BlueXP 에 NSS 계정을 추가합니다.

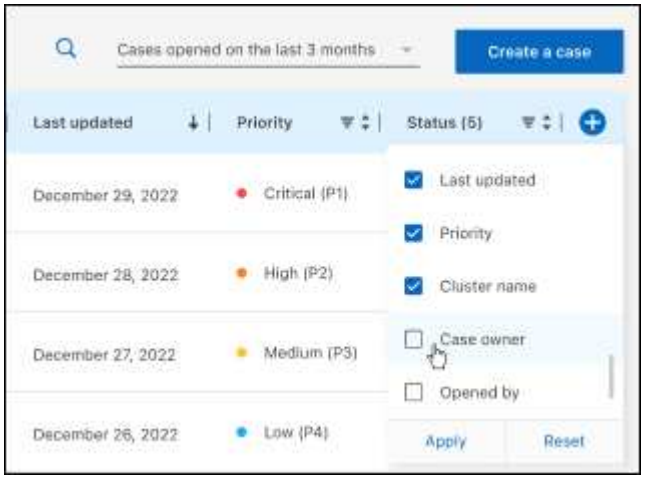
   사례 관리 페이지는 BlueXP 사용자 계정과 연결된 NSS 계정과 관련된 미해결 사례를 보여줍니다. 이는 **NSS** 관리 페이지 상단에 표시되는 NSS 계정과 동일합니다.
3. 필요에 따라 표에 표시되는 정보를 수정합니다.
   - *조직 사례*에서 *보기*를 선택하면 회사와 관련된 모든 사례를 볼 수 있습니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정하세요.



◦ 열의 내용을 필터링합니다.



◦ 표에 나타나는 열을 변경하려면 다음을 선택하세요. 그런 다음 표시하려는 열을 선택합니다.

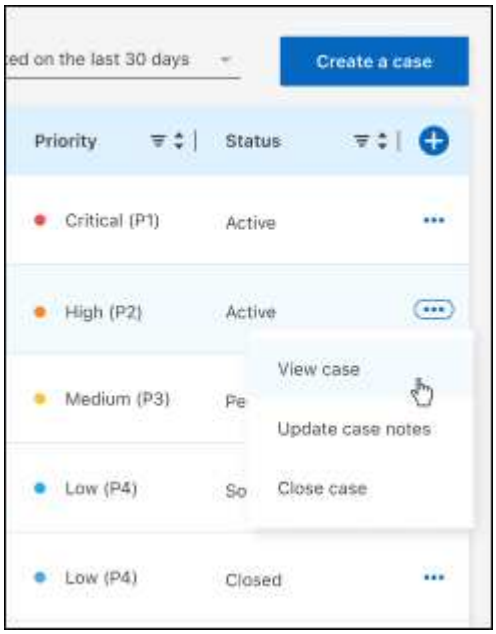


4. 기존 사례를 관리하려면 다음을 선택하세요. 그리고 사용 가능한 옵션 중 하나를 선택하세요:

- 사례 보기: 특정 사례에 대한 전체 세부 정보를 확인하세요.
- 사례 메모 업데이트: 문제에 대한 추가 세부 정보를 제공하거나 *파일 업로드*를 선택하여 최대 5개의 파일을 첨부하세요.

  첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.

- 사건 종결: 사건을 종결하는 이유를 자세히 입력하고 *사건 종결*을 선택하세요.



법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인정보 보호정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈소스

공지 파일은 NetApp 소프트웨어에서 사용되는 타사 저작권 및 라이선스에 대한 정보를 제공합니다.

"NetApp 복사 및 동기화에 대한 알림"

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.