NetApp Copy and Syncのドキュメント

NetApp Copy and Sync

NetApp
December 16, 2025

目次

NetApp Copy and Syncのドキュメント 1
リリース ノート 2
NetApp Copy and Syncの新機能 2
2025年10月6日 2
2025年2月2日 2
2024年10月27日 2
2024年9月16日 2
2024年8月11日 2
2024年7月14日 3
2024年6月2日 3
2024年4月8日 3
2024年2月11日 3
2023年11月26日 3
2023年9月3日 4
2023年8月6日 4
2023年7月9日 5
2023年6月11日 5
2023年5月8日 5
2023年4月2日 6
2023年3月7日 6
2023年2月5日 6
2023年1月3日 7
2022年12月11日 7
2022年10月30日 8
2022年9月4日 8
2022年7月31日 9
2022年7月3日 10
2022年6月6日 12
2022年5月1日 13
2022年4月3日 13
2022年3月3日 14
2022年2月6日 15
2022年1月2日 16
2021年11月28日 18
2021年10月31日 19
2021年10月4日 19
2021年9月2日 19
2021年8月1日 20
2021年7月7日 21

2021年6月7日 22
2021年5月2日 22
2021年4月11日 22
NetApp Copy and Syncの制限 23
始めましょう 25
NetApp Copy and Syncについて学ぶ 25
NetApp Console 25
NetApp Copy and Syncの仕組み 25
サポートされているストレージ タイプ 26
費用 27
NetApp Copy and Syncのクイックスタート 27
NetApp Copy and Syncでサポートされている同期関係 28
NetApp Copy and Syncでソースとターゲットを準備する 36
ネットワーク 36
ターゲット ディレクトリ 36
ディレクトリの読み取り権限 37
Amazon S3バケットの要件 37
Azure Blobストレージの要件 38
Azure データレイクストレージ Gen2 40
Azure NetApp Files の要件 40
ボックスの要件 41
Google Cloud Storage バケットの要件 41
Googleドライブ 42
NFSサーバの要件 42
ONTAPの要件 43
ONTAP S3 ストレージ要件 43
SMBサーバの要件 43
NetApp Copy and Syncのネットワーク概要 44
データブローカーの場所 44
ネットワーク要件 45
ネットワークエンドポイント 45
NetApp Copy and Syncにログイン 47
データブローカーをインストールする 48
NetApp Copy and Sync用の新しいデータブローカーを AWS に作成する 48
Azure でNetApp Copy and Sync用の新しいデータ ブローカーを作成する 51
Google Cloud でNetApp Copy and Sync用の新しいデータ ブローカーを作成する 57
NetApp Copy and Sync用のデータ ブローカーを Linux ホストにインストールします。 62
NetApp Copy and Syncを使用する 67
ソースとターゲット間でデータを同期する 67
NetApp Copy and Syncのオブジェクト ストレージ間でデータを同期するためのデータ ブローカーを準備します。 67

NetApp Copy and Syncで同期関係を作成する 67
NetApp Copy and Syncで SMB 共有から ACL をコピーする 76
NetApp Copy and Syncの Data In Flight 暗号化を使用して NFS データを同期する 78
NetApp Copy and Syncで外部 HashiCorp Vault を使用するためのデータ ブローカー グループを設定する 82
NetApp Copy and Syncの無料トライアル期間終了後は、同期関係の料金が発生します。 88
AWSからサブスクライブ 88
Azureからサブスクライブ 88
NetAppからライセンスを購入し、コピーと同期に追加します 89
ライセンスを更新する 90
NetApp Copy and Syncでの同期関係の管理 90
即時データ同期を実行する 90
同期パフォーマンスを高速化 90
資格情報を更新する 91
通知を設定する 92
同期関係の設定を変更する 93
関係を削除する 97
NetApp Copy and Syncでデータブローカーグループを管理する 97
データブローカーグループの仕組み 97
セキュリティに関する推奨事項 98
グループに新しいデータブローカーを追加する 98
グループの名前を編集する 99
統一された構成を設定する 100
データブローカーをグループ間で移動する 101
プロキシ設定を更新する 101
データブローカーの構成を表示する 102
データブローカーの問題に対処する 103
グループからデータブローカーを削除する 104
データブローカーグループを削除する 104
NetApp Copy and Syncで構成を調整するためのレポートを作成して表示します 105
レポートを作成する 105
レポートをダウンロード 107
レポートエラーを表示 108
レポートを削除する 108
NetApp Copy and Syncのデータブローカーをアンインストールする 109
NetApp Copy and SyncAPI 110
始めましょう 110
リストAPIを使用する 111
APIリファレンス 113
概念 114
NetApp Copy and Syncのライセンスの概要 114

マーケットプレイスサブスクリプション 114
NetAppのライセンス 114
NetApp Copy and Syncにおけるデータプライバシー 115
NetApp Copy and Sync技術 FAQ 115
開始 115
サポートされているソースとターゲット 117
ネットワーク 118
データ同期 118
セキュリティ 119
権限 120
オブジェクトストレージメタデータ 120
パフォーマンス 121
削除する 122
トラブルシューティング 122
データブローカーの詳細 122
知識とサポート 124
サポートに登録する 124
サポート登録の概要 124
NetAppサポートのためにNetApp Consoleを登録する 124
Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける 126
ヘルプを受ける 128
クラウドプロバイダーのファイルサービスのサポートを受ける 128
セルフサポートオプションを使用する 128
NetAppサポートでケースを作成する 128
サポートケースを管理する（プレビュー） 131
法律上の表示 134
著作権 134
商標 134
特許 134
プライバシー ポリシー 134
オープンソース 134

NetApp Copy and Syncのドキュメント

リリース ノート

NetApp Copy and Syncの新機能

NetApp Copy and Syncの新機能について説明します。

2025年10月6日

BlueXP copy and syncは**NetApp Copy and Sync**になりました

BlueXP copy and syncは、 NetApp Copy and Syncに名前が変更されました。

BlueXPは**NetApp Console**になりました

NetApp Consoleは、強化され再構築されたBlueXP基盤上に構築され、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとNetApp Data Servicesの集中管理を提供し、リアルタイムの分析情報、より高速なワークフロー、および高度なセキュリティとコンプライアンスを備えた簡素化された管理を実現します。

変更内容の詳細については、"NetApp Consoleのリリースノート" 。

2025年2月2日

データブローカーの新しい**OS**サポート

データ ブローカーは、Red Hat Enterprise 9.4、Ubuntu 23.04、Ubuntu 24.04 を実行しているホストでサポートされるようになりました。

"Linuxホストの要件を表示" 。

2024年10月27日

バグ修正

いくつかのバグを修正するために、 NetApp Copy and Syncとデータ ブローカーを更新しました。新しいデータ ブローカーのバージョンは 1.0.56 です。

2024年9月16日

バグ修正

いくつかのバグを修正するために、 NetApp Copy and Syncとデータ ブローカーを更新しました。新しいデータ ブローカーのバージョンは 1.0.55 です。

2024年8月11日

バグ修正

いくつかのバグを修正するために、 NetApp Copy and Syncとデータ ブローカーを更新しました。新しいデータ ブローカーのバージョンは 1.0.54 です。

2024年7月14日

バグ修正

いくつかのバグを修正するために、コピーと同期およびデータ ブローカーを更新しました。新しいデータ ブローカーのバージョンは 1.0.53 です。

2024年6月2日

バグ修正

NetApp Copy and Syncが更新され、いくつかのバグが修正されました。データ ブローカーも更新され、セキュリティ更新が適用されます。新しいデータ ブローカーのバージョンは 1.0.52 です。

2024年4月8日

RHEL 8.9 のサポート

データ ブローカーは、Red Hat Enterprise Linux 8.9 を実行しているホストでサポートされるようになりました。

"Linuxホストの要件を表示" 。

2024年2月11日

正規表現でディレクトリをフィルタリングする

ユーザーは正規表現を使用してディレクトリをフィルタリングできるようになりました。

"*ディレクトリを除外*機能の詳細をご覧ください。"

2023年11月26日

Azure Blob のコールド ストレージ クラスのサポート

同期関係を作成するときに、コールド ストレージ Azure Blob 層が使用できるようになりました。

"同期関係の作成について詳しく学習します。"

AWS データブローカーにおけるテルアビブリージョンのサポート

AWS でデータブローカーを作成するときに、テルアビブがサポートされるリージョンになりました。

"AWSでデータブローカーを作成する方法の詳細" 。

データブローカーのノードバージョンの更新

すべての新しいデータ ブローカーは、ノード バージョン 21.2.0 を使用します。 CentOS 7.0 や Ubuntu Server 18.0 など、このアップデートと互換性のないデータ ブローカーは、 NetApp Copy and Syncで動作しなくなります。

2023年9月3日

正規表現でファイルを除外する

ユーザーは正規表現を使用してファイルを除外できるようになりました。

"*ファイル拡張子を除外*機能の詳細をご覧ください。"

Azure データブローカーの作成時に **S3** キーを追加する

ユーザーは、Azure データ ブローカーを作成するときに、AWS S3 アクセス キーと秘密キーを追加できるようになりました。

"Azure でデータ ブローカーを作成する方法の詳細について説明します。"

2023年8月6日

データ ブローカーを作成するときに既存の **Azure** セキュリティ グループを使用する

ユーザーは、データ ブローカーを作成するときに、既存の Azure セキュリティ グループを使用するオプションを利用できるようになりました。

データ ブローカーの作成時に使用するサービス アカウントには、次の権限が必要です。

- 「Microsoft.Network/ネットワークセキュリティグループ/セキュリティルール/読み取り」
- 「Microsoft.Network/networkSecurityGroups/読み取り」

"Azure でデータ ブローカーを作成する方法の詳細について説明します。"

Google ストレージに同期するときにデータを暗号化する

ユーザーは、Google ストレージ バケットをターゲットとして同期関係を作成するときに、顧客管理の暗号化キーを指定できるようになりました。キーを手動で入力するか、単一のリージョン内のキーのリストから選択することができます。

データ ブローカーの作成時に使用するサービス アカウントには、次の権限が必要です。

- cloudkms.cryptoKeys.リスト
- cloudkms.keyRings.リスト

"Google Cloud Storage バケットの要件の詳細をご覧ください。"

2023年7月9日

複数の同期関係を一度に削除する

ユーザーは UI で一度に複数の同期関係を削除できるようになりました。

"同期関係の削除の詳細について説明します。"

ACLのみコピー

ユーザーには、CIF および NFS 関係で ACL 情報をコピーするための追加オプションが提供されるようになりました。同期関係を作成または管理するときに、ファイルのみをコピーしたり、ACL 情報のみをコピーしたり、ファイルと ACL 情報をコピーしたりできます。

"ACL のコピーについて詳しく学びます。"

Node.js 20にアップデート

コピーと同期が Node.js 20 に更新されました。利用可能なすべてのデータ ブローカーが更新されます。この更新プログラムと互換性のないオペレーティング システムはインストールできず、互換性のない既存のシステムではパフォーマンスの問題が発生する可能性があります。

2023年6月11日

分単位の自動中止をサポート

完了していないアクティブな同期は、*同期タイムアウト*機能を使用して 15 分後に中止できるようになりました。

"同期タイムアウト設定の詳細" 。

アクセス時間メタデータをコピーする

ファイル システムを含む関係では、*オブジェクトのコピー*機能によってアクセス時間のメタデータがコピーされるようになりました。

"オブジェクトのコピー設定の詳細" 。

2023年5月8日

ハードリンク機能

ユーザーは、セキュリティ保護されていない NFS と NFS の関係を含む同期にハード リンクを含めることができるようになりました。

"ファイルタイプの設定について詳しくは" 。

セキュア **NFS** 関係におけるデータ ブローカーのユーザー証明書を追加する機能

ユーザーは、安全な NFS 関係を作成するときに、ターゲット データ ブローカーに対して独自の証明書を設定できるようになりました。その際、サーバー名を設定し、秘密鍵と証明書 ID を提供する必要があります。

この機能は、すべてのデータ ブローカーで利用できます。

最近変更されたファイルの除外期間の延長

ユーザーは、スケジュールされた同期の最大 365 日前までに変更されたファイルを除外できるようになりました。

"最近変更されたファイルの設定について詳しくは" 。

UI で関係 **ID** による関係のフィルタリング

RESTful API を使用しているユーザーは、関係 ID を使用して関係をフィルターできるようになりました。

"NetApp Copy and Syncで RESTful API を使用する方法の詳細" 。

"除外ディレクトリ設定の詳細" 。

2023年4月2日

Azure Data Lake Storage Gen2 関係の追加サポート

次のようにして、Azure Data Lake Storage Gen2 をソースおよびターゲットとして同期関係を作成できるようになりました。

- Azure NetApp Files
- Amazon FSx for ONTAP
- Cloud Volumes ONTAP
- オンプレミスONTAP

"サポートされている同期関係の詳細" 。

フルパスでディレクトリをフィルタリングする

名前によるディレクトリのフィルタリングに加えて、フルパスによるディレクトリのフィルタリングも可能になりました。

"除外ディレクトリ設定の詳細" 。

2023年3月7日

AWS データブローカー向け **EBS** 暗号化

アカウントの KMS キーを使用して AWS データブローカーボリュームを暗号化できるようになりました。

"AWSでデータブローカーを作成する方法の詳細" 。

2023年2月5日

Azure Data Lake Storage Gen2、 **ONTAP S3** ストレージ、**NFS** の追加サポート

Cloud Sync は、 ONTAP S3 ストレージと NFS の追加の同期関係をサポートするようになりました。

- ONTAP S3 ストレージから NFS へ
- NFS からONTAP S3 ストレージへ

Cloud Syncでは、Azure Data Lake Storage Gen2 をソースとターゲットの両方としてサポートし、次のことが可能になります。

- NFS サーバ
- SMB サーバ
- ONTAP S3 ストレージ
- StorageGRID
- IBM Cloud Object Storage

"サポートされている同期関係の詳細" 。

Amazon Web Services データブローカー オペレーティング システムへのアップグレード

AWS データブローカーのオペレーティングシステムが Amazon Linux 2022 にアップグレードされました。

"AWS のデータブローカーインスタンスの詳細" 。

2023年1月3日

UI にデータ ブローカーのローカル構成を表示する

ユーザーが UI 上で各データ ブローカーのローカル構成を表示できる 構成の表示 オプションが追加されました。

"データブローカーグループの管理の詳細" 。

Azure および **Google Cloud** データ ブローカー オペレーティング システムへのアップグレード

Azure および Google Cloud のデータ ブローカーのオペレーティング システムが Rocky Linux 9.0 にアップグレードされました。

"Azure のデータ ブローカー インスタンスの詳細" 。

"Google Cloud のデータブローカーインスタンスの詳細" 。

2022年12月11日

名前でディレクトリをフィルタリングする

同期関係に新しい ディレクトリ名を除外 設定が利用できるようになりました。ユーザーは、同期から最大 15 個のディレクトリ名を除外できます。デフォルトでは、.copy-offload、.snapshot、~snapshot ディレクトリは除外されます。

"ディレクトリ名を除外する設定の詳細" 。

追加の **Amazon S3** および**ONTAP S3** ストレージのサポート

Cloud Sync は、AWS S3 およびONTAP S3 ストレージの追加の同期関係をサポートするようになりました。

- AWS S3 からONTAP S3 ストレージへ
- ONTAP S3 ストレージから AWS S3 へ

"サポートされている同期関係の詳細" 。

2022年10月30日

Microsoft Azureからの継続的な同期

Azure データ ブローカーを使用して、ソース Azure ストレージ バケットからクラウド ストレージへの継続的な同期設定がサポートされるようになりました。

最初のデータ同期の後、 Cloud Sync はソースの Azure ストレージ バケットの変更をリッスンし、変更が発生するたびにターゲットに継続的に同期します。この設定は、Azure ストレージ バケットから Azure Blob ストレージ、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、 StorageGRIDに同期するときに使用できます。

この設定を使用するには、Azure データ ブローカーにカスタム ロールと次のアクセス許可が必要です。

```
'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'
```

"継続同期設定の詳細" 。

2022年9月4日

Googleドライブの追加サポート

- Cloud Sync は、 Google ドライブの追加の同期関係をサポートするようになりました。
  - Google ドライブから NFS サーバーへ
  - Google ドライブから SMB サーバーへ

- Google ドライブを含む同期関係のレポートを生成することもできます。

  "レポートの詳細" 。

継続的な同期の強化

次の種類の同期関係で継続的な同期設定を有効にできるようになりました。

- S3バケットからNFSサーバーへ
- Google Cloud Storage から NFS サーバーへ

"継続同期設定の詳細" 。

メール通知

Cloud Sync の通知を電子メールで受信できるようになりました。

電子メールで通知を受信するには、同期関係で 通知 設定を有効にし、 NetApp Consoleでアラートと通知の設定を構成する必要があります。

"通知の設定方法を学ぶ" 。

2022年7月31日

Googleドライブ

NFS サーバーまたは SMB サーバーから Google ドライブにデータを同期できるようになりました。 「マイドライブ」と「共有ドライブ」の両方がターゲットとしてサポートされています。

Google ドライブを含む同期関係を作成するには、必要な権限と秘密鍵を持つサービス アカウントを設定する必要があります。 "Googleドライブの要件について詳しくは" 。

"サポートされている同期関係のリストを表示する" 。

追加の **Azure Data Lake** サポート

Cloud Sync は、Azure Data Lake Storage Gen2 の追加の同期関係をサポートするようになりました。

- Amazon S3 から Azure Data Lake Storage Gen2 へ
- IBM Cloud Object Storage から Azure Data Lake Storage Gen2 へ
- StorageGRIDから Azure Data Lake Storage Gen2 へ

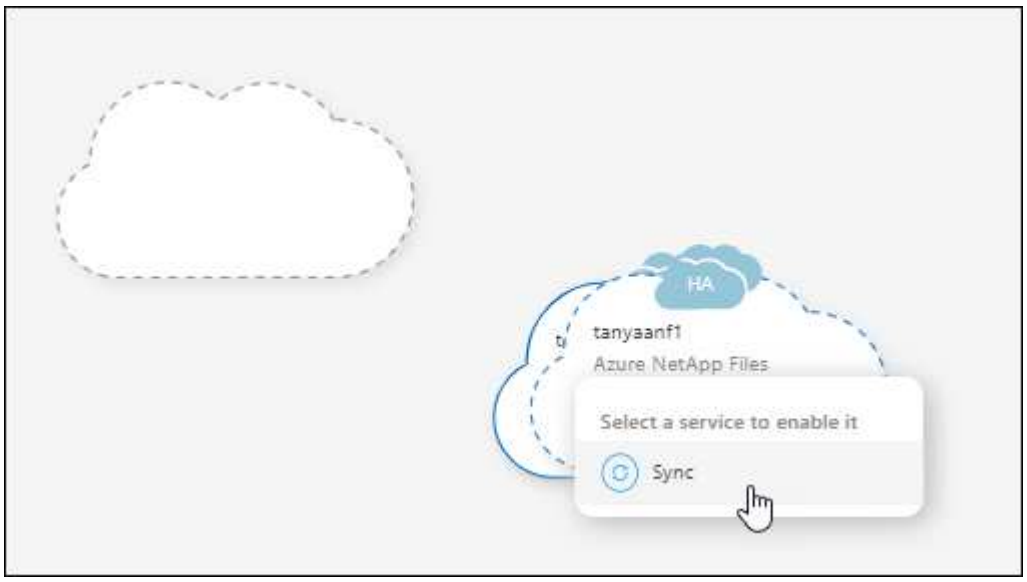
"サポートされている同期関係のリストを表示する" 。

同期関係を設定する新しい方法

NetAppコンソールのシステム ページから直接同期関係を設定するための追加の方法が追加されました。

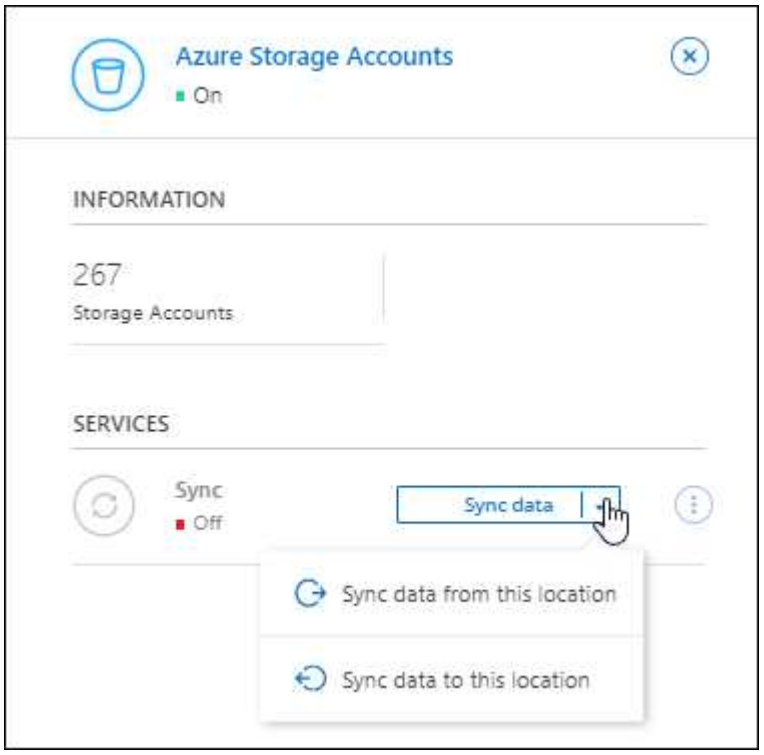
ドラッグ アンド ドロップ

システム ページから、あるシステムを別のシステムの上にドラッグ アンド ドロップすることで、同期関係を設定できるようになりました。



右パネルのセットアップ

システム ページからシステムを選択し、右側のパネルから同期オプションを選択することで、Azure Blob Storage または Google Cloud Storage の同期関係を設定できるようになりました。



2022年7月3日

Azure Data Lake Storage Gen2 のサポート

NFS サーバーまたは SMB サーバーから Azure Data Lake Storage Gen2 にデータを同期できるようになりました。

Azure Data Lake を含む同期関係を作成する場合は、 Cloud Syncにストレージ アカウント接続文字列を提供する必要があります。共有アクセス署名 (SAS) ではなく、通常の接続文字列である必要があります。

"サポートされている同期関係のリストを表示する" 。

Google Cloud Storageからの継続的な同期

ソースの Google Cloud Storage バケットからクラウド ストレージ ターゲットへの継続的な同期設定がサポートされるようになりました。

最初のデータ同期の後、 Cloud Sync はソースの Google Cloud Storage バケットの変更をリッスンし、変更が発生するたびにターゲットに継続的に同期します。この設定は、Google Cloud Storage バケットから S3 、Google Cloud Storage、Azure Blob Storage、 StorageGRID、または IBM Storage に同期するときに使用できます。

この設定を使用するには、データ ブローカーに関連付けられたサービス アカウントに次の権限が必要です。

```
- 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
```

"継続同期設定の詳細" 。

新しい Google Cloud リージョンのサポート

Cloud Syncデータ ブローカーは、次の Google Cloud リージョンでサポートされるようになりました。

- コロンバス（米国東部5）
- ダラス（米国南部1）
- マドリード（ヨーロッパ南西部1）
- ミラノ（ヨーロッパ西8）
- パリ（ヨーロッパ西9）

新しい **Google Cloud** マシンタイプ

Google Cloud のデータ ブローカーのデフォルトのマシンタイプは n2-standard-4 になりました。

2022年6月6日

連続同期

新しい設定により、ソース S3 バケットからターゲットへの変更を継続的に同期できるようになります。

最初のデータ同期の後、 Cloud Sync はソースの S3 バケットの変更をリッスンし、変更が発生するたびにターゲットに継続的に同期します。スケジュールされた間隔でソースを再スキャンする必要はありません。この設定は、S3 バケットから S3、Google Cloud Storage、Azure Blob Storage、 StorageGRID、または IBM Storage に同期する場合にのみ使用できます。

この設定を使用するには、データ ブローカーに関連付けられた IAM ロールに次の権限が必要であることに注意してください。

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

これらの権限は、作成する新しいデータ ブローカーに自動的に追加されます。

"継続同期設定の詳細" 。

すべての**ONTAP**ボリュームを表示

同期関係を作成すると、 Cloud Sync はソースのCloud Volumes ONTAPシステム、オンプレミスのONTAPクラスター、または FSx for ONTAPファイル システム上のすべてのボリュームを表示するようになりました。

以前は、 Cloud Sync、選択したプロトコルに一致するボリュームのみが表示されていました。これですべてのボリュームが表示されますが、選択したプロトコルと一致しないボリュームや共有またはエクスポートがないボリュームはグレー表示され、選択できなくなります。

Azure Blob へのタグのコピー

Azure Blob をターゲットとする同期関係を作成すると、 Cloud Syncでは Azure Blob コンテナーにタグをコピーできるようになりました。

- 設定 ページで、オブジェクトのコピー 設定を使用して、ソースから Azure BLOB コンテナーにタグをコピーできます。これはメタデータのコピーに加えて行われます。
- タグ/メタデータ ページでは、Azure BLOB コンテナーにコピーされるオブジェクトに設定する BLOB インデックス タグを指定できます。以前は、関係メタデータのみを指定できました。

これらのオプションは、Azure Blob がターゲットであり、ソースが Azure Blob または S3 互換エンドポイント (S3、 StorageGRID、または IBM Cloud Object Storage) のいずれかである場合にサポートされます。

2022年5月1日

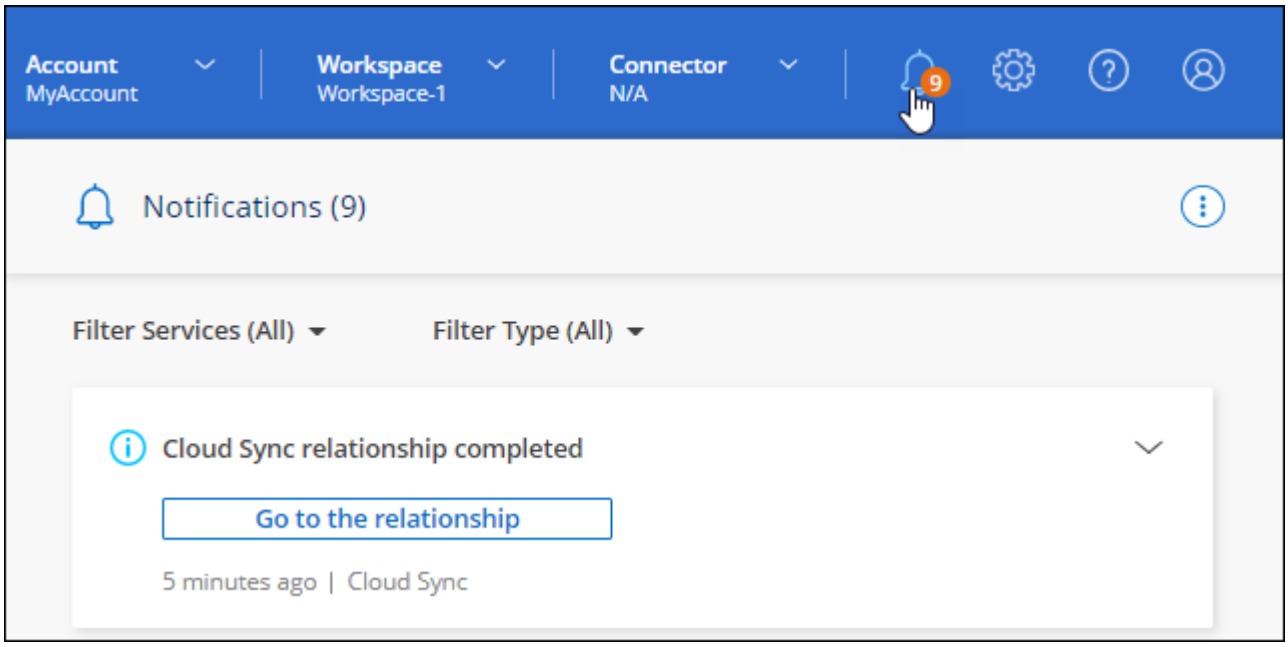
同期タイムアウト

同期関係に新しい 同期タイムアウト 設定が利用できるようになりました。この設定では、指定された時間数または日数内に同期が完了しなかった場合に、 Cloud Sync がデータ同期をキャンセルするかどうかを定義できます。

"同期関係の設定の変更について詳しくは、こちらをご覧ください。" 。

通知

同期関係に新しい 通知 設定が利用できるようになりました。この設定により、 NetAppコンソールの通知センターでCloud Sync通知を受信するかどうかを選択できます。成功したデータ同期、失敗したデータ同期、キャンセルされたデータ同期に関する通知を有効にすることができます。



"同期関係の設定の変更について詳しくは、こちらをご覧ください。" 。

2022年4月3日

データブローカーグループの機能強化

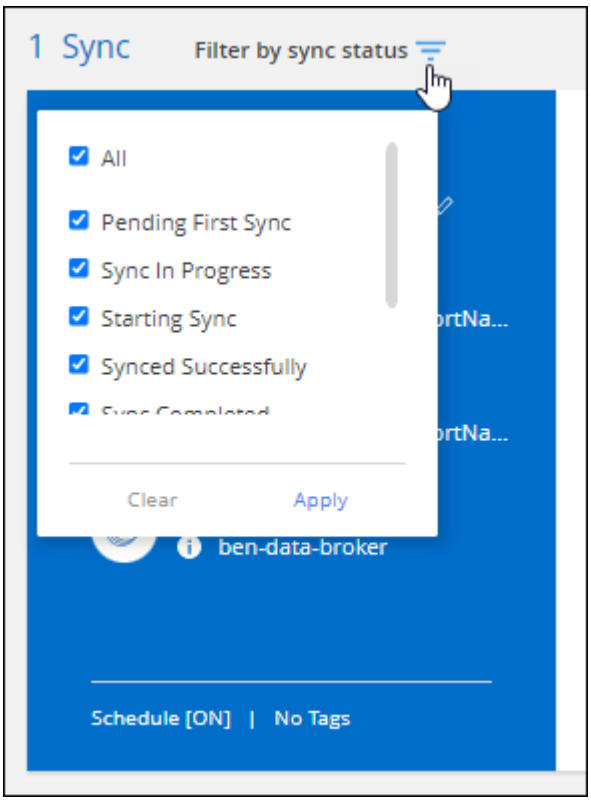
データ ブローカー グループにいくつかの機能強化を加えました。

- データ ブローカーを新規または既存のグループに移動できるようになりました。
- データ ブローカーのプロキシ構成を更新できるようになりました。
- 最後に、データ ブローカー グループを削除することもできます。

"データブローカーグループの管理方法を学ぶ" 。

ダッシュボードフィルター

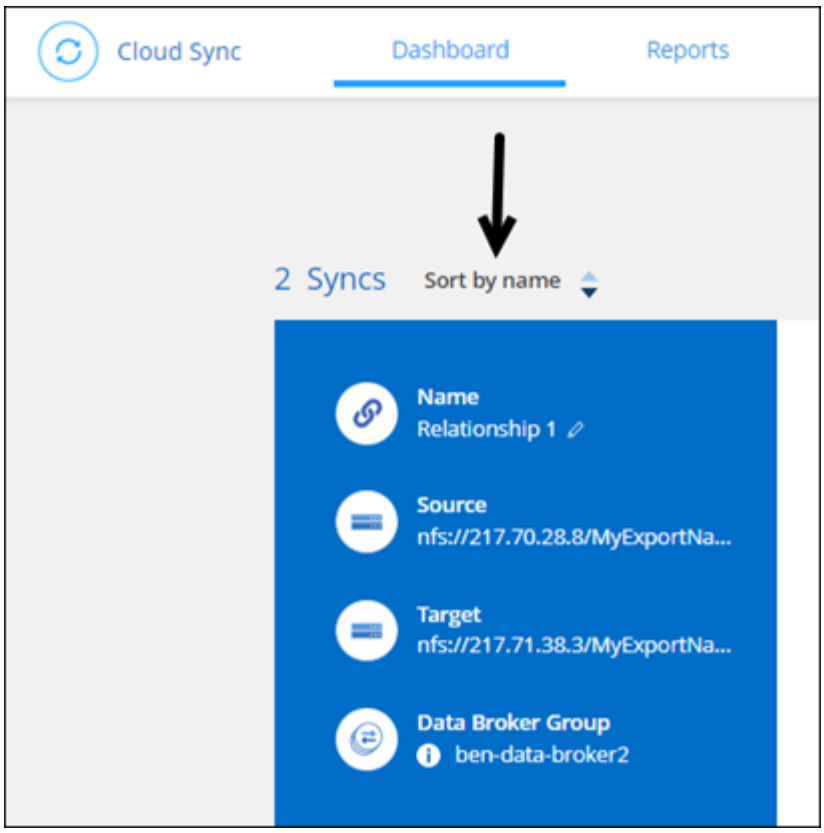
同期ダッシュボードの内容をフィルタリングして、特定のステータスに一致する同期関係をより簡単に見つけることができるようになりました。たとえば、失敗したステータスの同期関係をフィルタリングすることができます



2022年3月3日

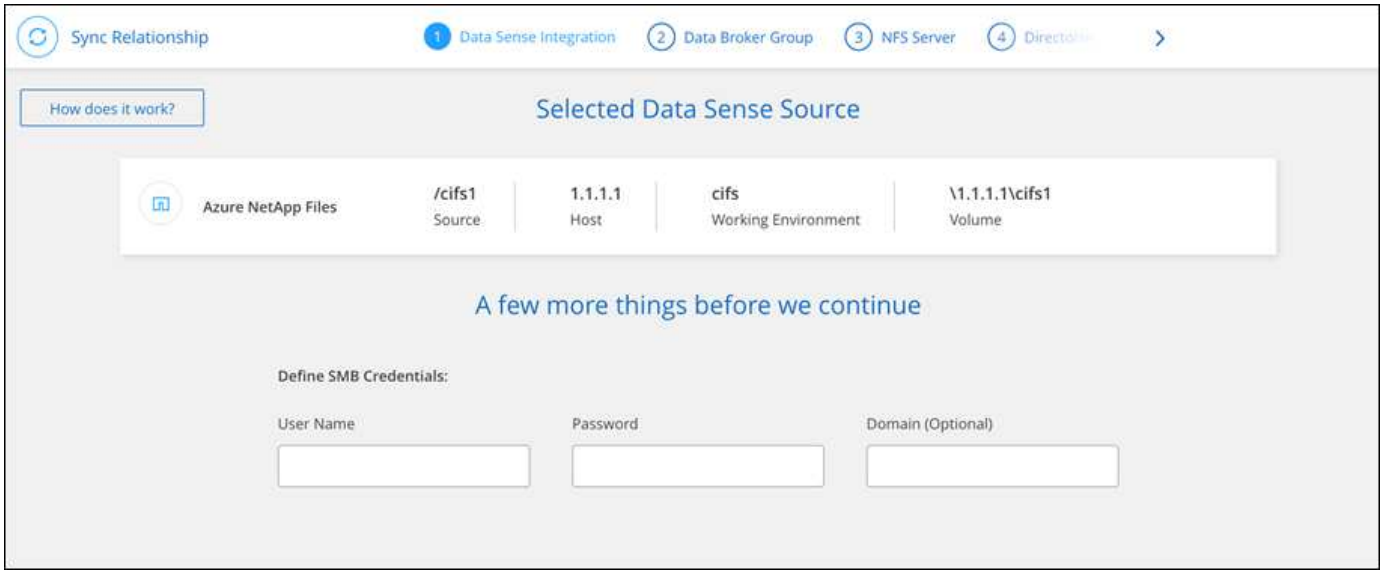
ダッシュボードでの並べ替え

ダッシュボードを同期関係名で並べ替えるようになりました。



Data Sense統合の強化

前回のリリースでは、 Cloud Syncと Cloud Data Sense の統合を導入しました。今回のアップデートでは、同期関係の作成が容易になり、統合が強化されました。 Cloud Data Sense からデータ同期を開始すると、すべてのソース情報が 1 つのステップにまとめられ、いくつかの重要な詳細を入力するだけで済みます。

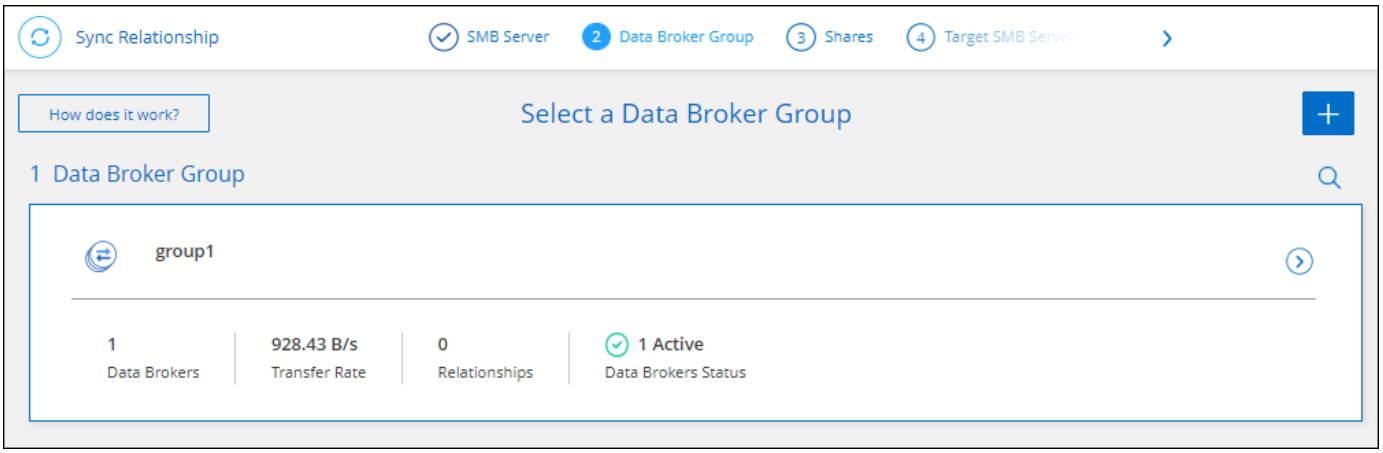


2022年2月6日

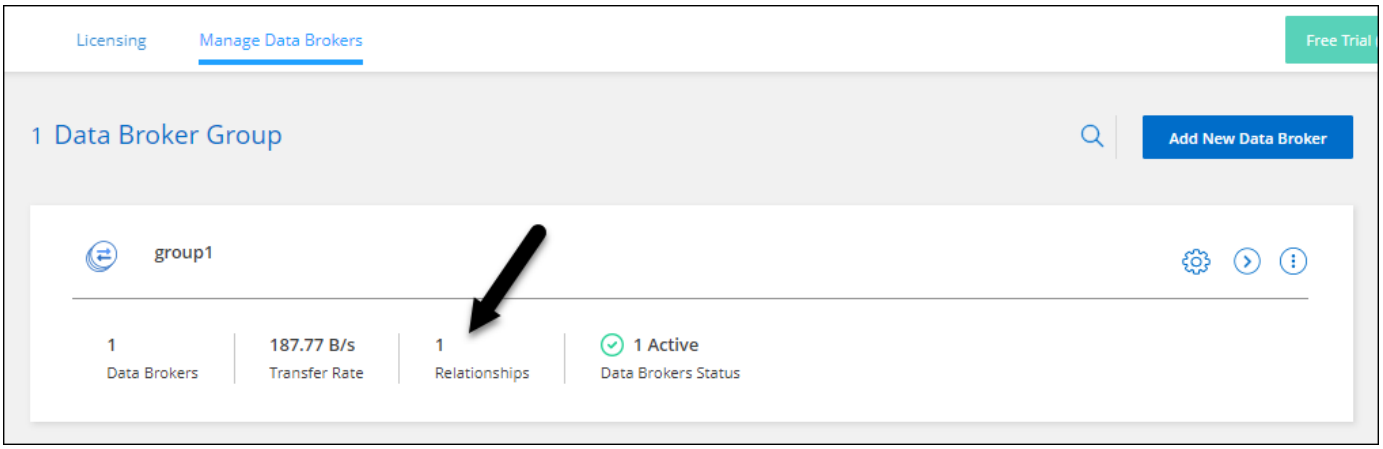
データブローカーグループの強化

データ ブローカー グループを強調することで、データ ブローカーとのやり取り方法を変更しました。

たとえば、新しい同期関係を作成するときは、特定のデータ ブローカーではなく、関係で使用するデータ ブローカー グループを選択します。



データ ブローカーの管理 タブには、データ ブローカー グループが管理している同期関係の数も表示されます。



PDFレポートをダウンロード

レポートの PDF をダウンロードできるようになりました。

"レポートの詳細" 。

2022年1月2日

新しい**Box**同期関係

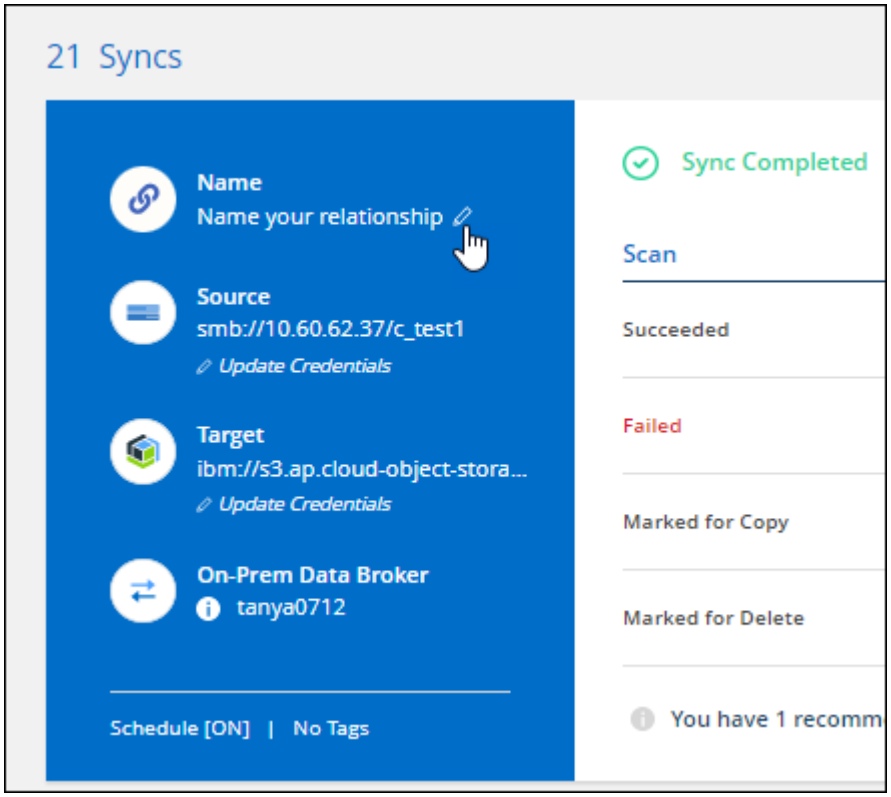
2 つの新しい同期関係がサポートされています。

- Box からAzure NetApp Filesへ
- Box からAmazon FSx for ONTAPへ

"サポートされている同期関係のリストを表示する" 。

関係名

各同期関係にわかりやすい名前を付けて、各関係の目的をより簡単に識別できるようになりました。関係を作成するときやその後いつでも名前を追加できます。



S3プライベートリンク

Amazon S3 との間でデータを同期するときに、S3 プライベートリンクを使用するかどうかを選択できます。データ ブローカーがソースからターゲットにデータをコピーする場合、プライベート リンクを経由します。

この機能を使用するには、データ ブローカーに関連付けられた IAM ロールに次の権限が必要であることに注意してください。

```
"ec2:DescribeVpcEndpoints"
```

この権限は、作成する新しいデータ ブローカーに自動的に追加されます。

氷河の即時検索

同期関係のターゲットが Amazon S3 の場合、*Glacier Instant Retrieval* ストレージ クラスを選択できるようになりました。

オブジェクトストレージから**SMB**共有への**ACL**

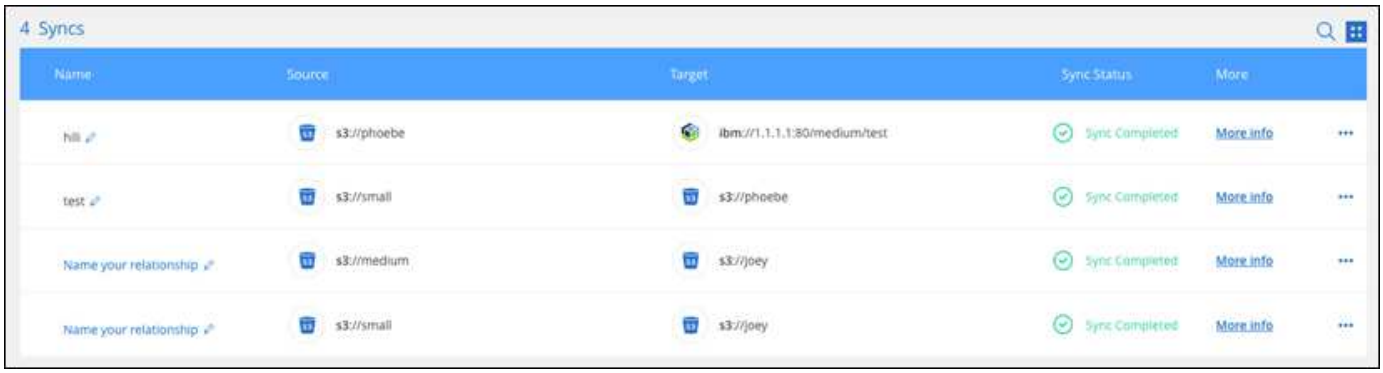
Cloud Syncでは、オブジェクト ストレージから SMB 共有への ACL のコピーがサポートされるようになりました。以前は、SMB 共有からオブジェクト ストレージへの ACL のコピーのみがサポートされていました。

SFTPから**S3**へ

SFTP から Amazon S3 への同期関係の作成がユーザー インターフェイスでサポートされるようになりました。この同期関係は以前は API でのみサポートされていました。

テーブルビューの強化

使いやすさを考慮して、ダッシュボードのテーブル ビューを再設計しました。 *詳細情報*を選択すると、Cloud Sync はダッシュボードをフィルターし、特定の関係に関する詳細情報を表示します。



ジャルカルタ地域への支援

Cloud Syncでは、AWS アジアパシフィック (ジャカルタ) リージョンでのデータブローカーのデプロイがサポートされるようになりました。

2021年11月28日

SMBからオブジェクトストレージへの**ACL**

Cloud Sync、ソース SMB 共有からオブジェクト ストレージ (ONTAP S3 を除く) への同期関係を設定するときに、アクセス制御リスト (ACL) をコピーできるようになりました。

Cloud Sync は、オブジェクト ストレージから SMB 共有への ACL のコピーをサポートしていません。

"SMB共有からACLをコピーする方法を学ぶ" 。

ライセンスの更新

延長したCloud Syncライセンスを更新できるようになりました。

NetAppから購入したCloud Syncライセンスを延長した場合は、ライセンスを再度追加して有効期限を更新できます。

"ライセンスの更新方法を学ぶ" 。

Boxの資格情報を更新する

既存の同期関係の Box 資格情報を更新できるようになりました。

"資格情報を更新する方法を学ぶ" 。

2021年10月31日

ボックスサポート

Box サポートが、 Cloud Syncユーザー インターフェースでプレビューとして利用できるようになりました。

Box は、いくつかの種類の同期関係においてソースまたはターゲットになることができます。"サポートされている同期関係のリストを表示する" 。

作成日の設定

SMB サーバーがソースの場合、「作成日」という新しい同期関係設定を使用すると、特定の日付以降、特定の日付前、または特定の時間範囲内に作成されたファイルを同期できます。

"Cloud Sync設定の詳細" 。

2021年10月4日

追加の**Box**サポート

Cloud Syncは、以下の追加の同期関係をサポートするようになりました。 "箱" Cloud Sync API を使用する場合:

- Amazon S3からBoxへ
- IBM Cloud Object StorageからBoxへ
- StorageGRIDからBoxへ
- BoxからNFSサーバーへ
- BoxからSMBサーバーへ

"APIを使用して同期関係を設定する方法を学びます" 。

SFTPパスのレポート

これで"レポートを作成する"SFTP パスの場合。

2021年9月2日

FSx for ONTAPのサポート

Amazon FSx for ONTAPファイルシステムとの間でデータを同期できるようになりました。

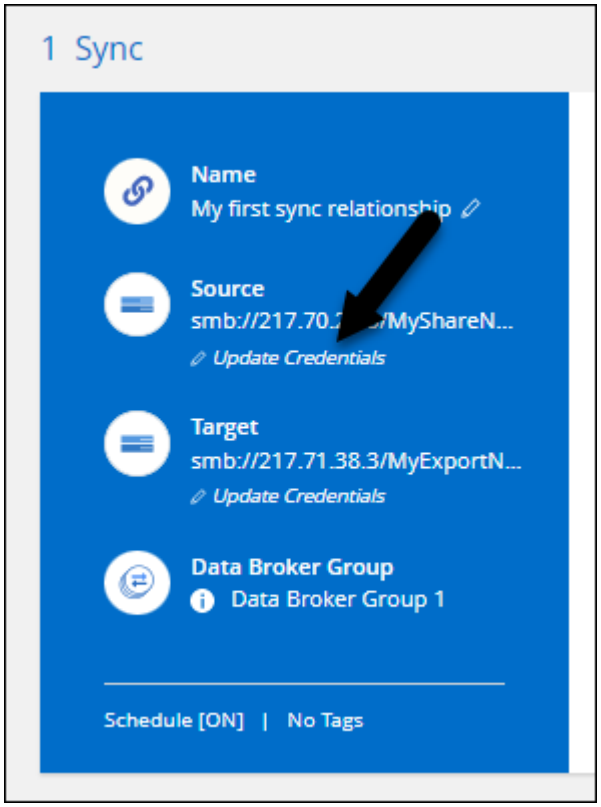
- "Amazon FSx for ONTAPについて学ぶ"
- "サポートされている同期関係を表示する"
- "Amazon FSx for ONTAPの同期関係を作成する方法を学びます"

2021年8月1日

資格情報を更新する

Cloud Syncでは、既存の同期関係のソースまたはターゲットの最新の資格情報を使用してデータ ブローカーを更新できるようになりました。

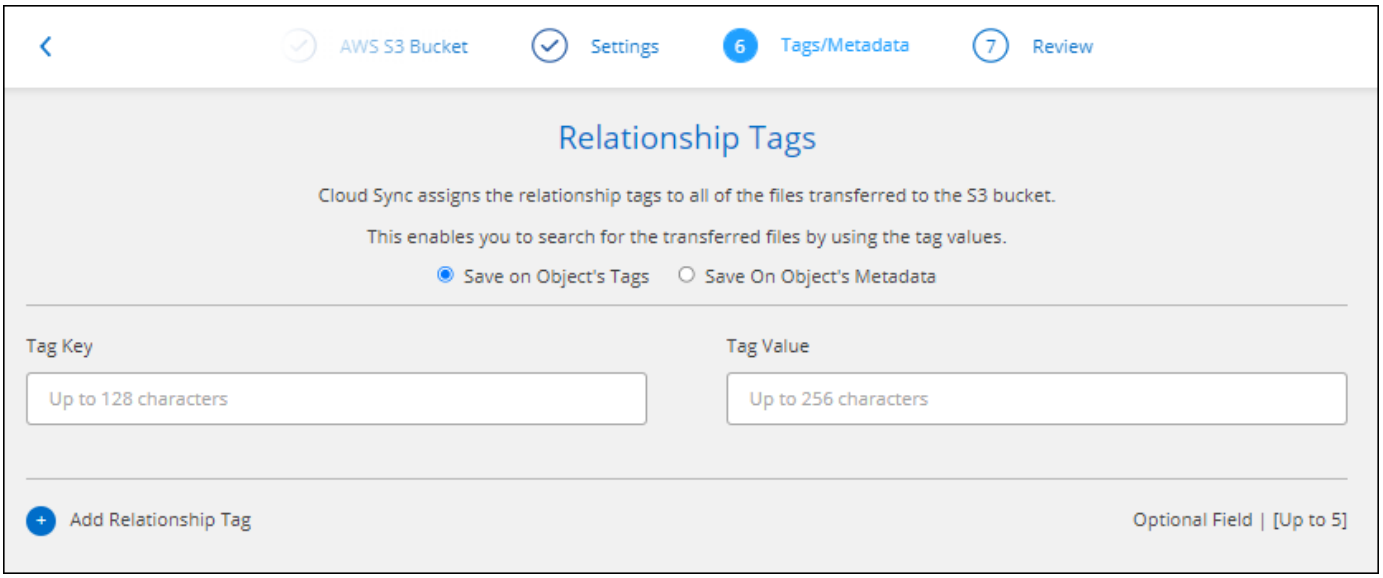
この機能強化は、セキュリティ ポリシーにより資格情報を定期的に更新する必要がある場合に役立ちます。"資格情報を更新する方法を学ぶ" 。



オブジェクトストレージターゲットのタグ

同期関係を作成するときに、同期関係のオブジェクト ストレージ ターゲットにタグを追加できるようになりました。

タグの追加は、Amazon S3、Azure Blob、Google Cloud Storage、IBM Cloud Object Storage、 StorageGRIDでサポートされています。



Boxのサポート

Cloud Syncがサポートされるようになりました "箱"Cloud Sync API を使用する場合、Amazon S3、StorageGRID 、IBM Cloud Object Storage との同期関係のソースとして。

"APIを使用して同期関係を設定する方法を学びます" 。

Google Cloud のデータ ブローカーのパブリック **IP**

Google Cloud にデータ ブローカーをデプロイするときに、仮想マシン インスタンスのパブリック IP アドレスを有効にするか無効にするかを選択できるようになりました。

"Google Cloud でデータブローカーをデプロイする方法を学びます" 。

Azure NetApp Filesのデュアルプロトコル ボリューム

Azure NetApp Filesのソース ボリュームまたはターゲット ボリュームを選択すると、同期関係にどのプロトコルを選択したかに関係なく、 Cloud Syncによってデュアル プロトコル ボリュームが表示されるようになりました。

2021年7月7日

ONTAP S3 ストレージと **Google Cloud** ストレージ

Cloud Sync は、ユーザー インターフェースからONTAP S3 ストレージと Google Cloud Storage バケット間の同期関係をサポートするようになりました。

"サポートされている同期関係のリストを表示する" 。

オブジェクトメタデータタグ

同期関係を作成し、設定を有効にすると、 Cloud Syncでオブジェクトベースのストレージ間でオブジェクトのメタデータとタグをコピーできるようになりました。

"オブジェクトのコピー設定の詳細" 。

HashiCorp Vaultsのサポート

Google Cloud サービス アカウントで認証することで、外部の HashiCorp Vault からの認証情報にアクセスするようにデータ ブローカーを設定できるようになりました。

"HashiCorp Vault をデータブローカーで使用する方法について詳しくは、こちらをご覧ください。" 。

S3バケットのタグまたはメタデータを定義する

Amazon S3 バケットとの同期関係を設定するときに、同期関係ウィザードを使用して、ターゲット S3 バケット内のオブジェクトに保存するタグまたはメタデータを定義できるようになりました。

タグ付けオプションは、以前は同期関係の設定の一部でした。

2021年6月7日

Google Cloud のストレージ クラス

Google Cloud Storage バケットが同期関係のターゲットである場合、使用するストレージ クラスを選択できるようになりました。 Cloud Sync は次のストレージ クラスをサポートしています。

- Standard
- ニアライン
- コールドライン
- アーカイブ

2021年5月2日

レポートのエラー

レポートで見つかったエラーを表示し、最後のレポートまたはすべてのレポートを削除できるようになりました。

"構成を調整するためのレポートの作成と表示について詳しくは、" 。

属性を比較する

各同期関係に対して、新しい 比較基準 設定が利用できるようになりました。

この詳細設定では、ファイルまたはディレクトリが変更されたかどうか、再度同期する必要があるかどうかを判断するときに、 Cloud Sync が特定の属性を比較するかどうかを選択できます。

"同期関係の設定の変更について詳しくは、こちらをご覧ください。" 。

2021年4月11日

スタンドアロンの**Cloud Sync**サービスは廃止されました

スタンドアロンのCloud Syncサービスは廃止されました。これで、 NetApp ConsoleからCloud Syncに直接アクセスし、同じ機能をすべて利用できるようになります。

NetApp Consoleにログインすると、上部の [同期] タブに切り替えて、以前と同じように関係を表示できます。

異なるプロジェクトの **Google Cloud** バケット

同期関係を設定するときに、データブローカーのサービス アカウントに必要な権限を付与すると、異なるプロジェクトの Google Cloud バケットから選択できます。

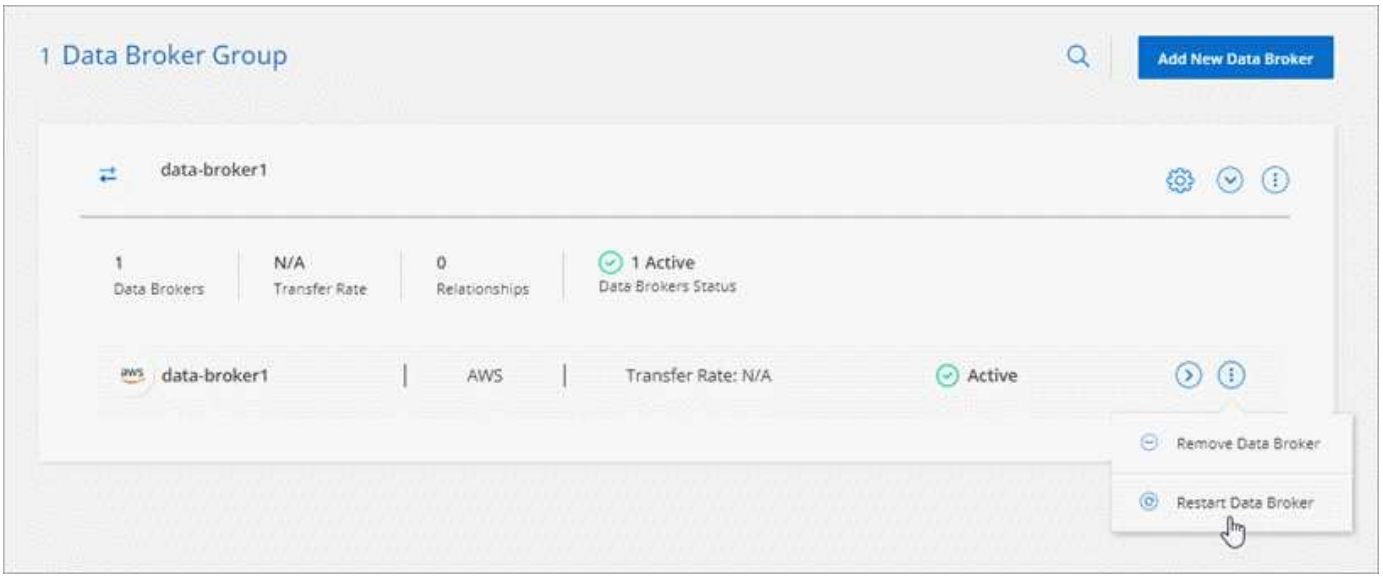
"サービスアカウントの設定方法を学ぶ" 。

Google Cloud Storage と **S3** 間のメタデータ

Cloud Syncでは、Google Cloud Storage と S3 プロバイダー (AWS S3、 StorageGRID、IBM Cloud Object Storage) 間でメタデータをコピーできるようになりました。

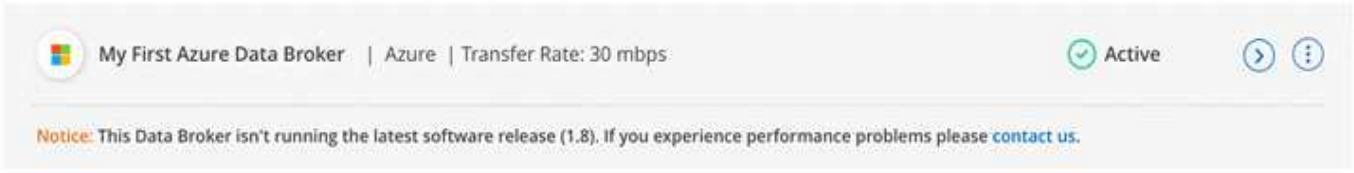
データブローカーを再起動する

Cloud Syncからデータ ブローカーを再起動できるようになりました。



最新リリースを実行していない場合のメッセージ

Cloud Sync、データ ブローカーが最新のソフトウェア リリースを実行していないことを識別できるようになりました。このメッセージは、最新の機能を確実に利用できるようにします。



NetApp Copy and Syncの制限

今回のリリースでサポートされていない、または今回のリリースでは正常に機能しない

プラットフォーム、デバイス、機能が記載されています。これらの制限事項をよく確認してください。

NetApp Copy and Sync は次のリージョンではサポートされていません。

- AWS 政府リージョン
- Azure Government リージョン
- 中国

始めましょう

NetApp Copy and Syncについて学ぶ

NetApp Copy and Sync は、クラウド内またはオンプレミスの任意のターゲットにデータを移行するためのシンプルで安全な自動化された方法を提供します。ファイルベースの NAS データセット (NFS または SMB)、Amazon Simple Storage Service (S3) オブジェクト形式、 NetApp StorageGRIDアプライアンス、またはその他のクラウド プロバイダー オブジェクト ストアのいずれであっても、Copy and Sync を使用すると変換して移動できます。

NetApp Console

NetApp Copy and Sync はNetApp Consoleからアクセスできます。

NetApp Consoleは、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとデータ サービスの集中管理を提供します。NetAppデータ サービスにアクセスして使用するには、コンソールが必要です。管理インターフェースとして、1 つのインターフェースから多数のストレージ リソースを管理できます。コンソール管理者は、企業内のすべてのシステムのストレージとサービスへのアクセスを制御できます。

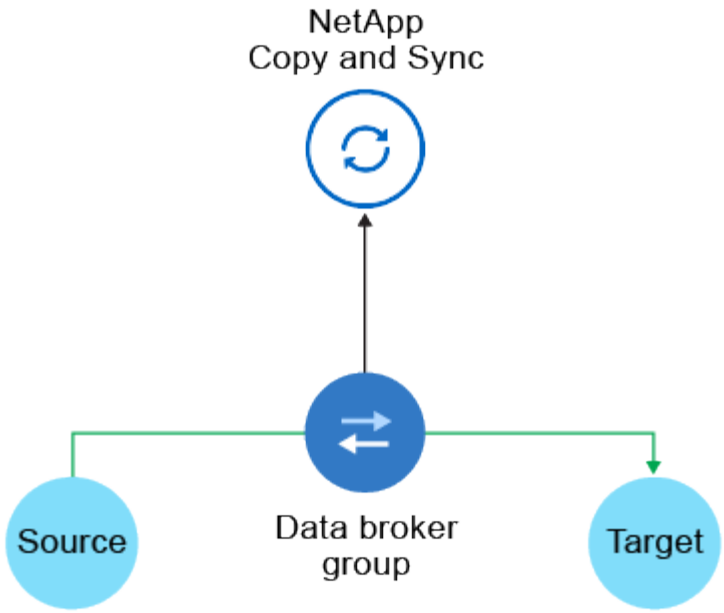
NetApp Consoleの使用を開始するためにライセンスやサブスクリプションは必要ありません。ストレージ システムまたはNetAppデータ サービスへの接続を確保するためにクラウドにコンソール エージェントを展開する必要がある場合にのみ料金が発生します。ただし、コンソールからアクセスできる一部のNetAppデータ サービスは、ライセンスまたはサブスクリプションベースです。

詳細はこちら "NetApp Console"。

NetApp Copy and Syncの仕組み

NetApp Copy and Sync は、データ ブローカー グループ、 NetApp Consoleから利用できるクラウドベースのインターフェイス、およびソースとターゲットで構成される SaaS (Software-as-a-Service) プラットフォームです。

次の図は、コピー コンポーネントと同期コンポーネントの関係を示しています。



NetAppデータ ブローカー ソフトウェアは、ソースからターゲットにデータを同期します (これを 同期関係 と呼びます)。データブローカーは、AWS、Azure、Google Cloud Platform、またはオンプレミスで実行できます。 1 つ以上のデータ ブローカーで構成されるデータ ブローカー グループには、Copy and Sync と通信し、他のいくつかのサービスやリポジトリに接続できるように、ポート 443 経由の送信インターネット接続が必要です。"エンドポイントのリストを表示する" 。

最初のコピーの後、コピーと同期は設定したスケジュールに基づいて変更されたデータを同期します。

サポートされているストレージ タイプ

コピーと同期は、次のストレージ タイプをサポートします。

- 任意のNFSサーバー
- 任意のSMBサーバー
- アマゾンEFS
- Amazon FSx for ONTAP
- Amazon S3
- Azure ブロブ
- Azure データレイクストレージ Gen2
- Azure NetApp Files
- ボックス（プレビューとして利用可能）
- Cloud Volumes ONTAP
- Google Cloud Storage
- Googleドライブ
- IBM Cloud Object Storage
- オンプレミスのONTAPクラスタ
- ONTAP S3 ストレージ

- SFTP（APIのみ使用）
- StorageGRID

"サポートされている同期関係を表示する" 。

費用

コピーと同期の使用に関連するコストには、リソース料金とサービス料金の 2 種類があります。

リソース料金

リソース料金は、クラウドで 1 つ以上のデータ ブローカーを実行するためのコンピューティング コストとストレージ コストに関連します。

サービス料

14 日間の無料トライアルが終了した後、同期関係の料金を支払う方法は 2 つあります。最初のオプションは、AWS または Azure からサブスクライブすることです。これにより、時間単位または年単位で支払いが可能になります。 2 番目のオプションは、 NetAppから直接ライセンスを購入することです。

"ライセンスの仕組みを学ぶ" 。

NetApp Copy and Syncのクイックスタート

NetApp Copy and Sync の使用を開始するには、いくつかの手順が必要です。

1 **NetApp Console**にログインして設定する

NetApp Consoleの使用を開始しているはずです。これには、ログイン、アカウントの設定、コンソール エージェントの展開、システムの作成などが含まれます。

次のいずれかの同期関係を作成する場合は、まずシステムを作成または検出する必要があります。

- Amazon FSx for ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- オンプレミスのONTAPクラスター

Cloud Volumes ONTAP、オンプレミスのONTAPクラスター、およびAmazon FSx for ONTAPには、コンソールエージェントが必要です。

- "NetApp Consoleの使い方を学ぶ"
- "コンソールエージェントの詳細"

2 ソースとターゲットを準備する

ソースとターゲットがサポートされ、設定されていることを確認します。最も重要な要件は、データ ブローカー グループとソースおよびターゲットの場所間の接続を確認することです。

- "サポートされている関係を表示する"
- "ソースとターゲットを準備する"

3 NetAppデータブローカーの場所を準備する

NetAppデータ ブローカー ソフトウェアは、ソースからターゲットにデータを同期します (これを 同期関係 と呼びます)。データブローカーは、AWS、Azure、Google Cloud Platform、またはオンプレミスで実行できます。 1 つ以上のデータ ブローカーで構成されるデータ ブローカー グループには、 NetApp Copy and Syncと通信し、他のいくつかのサービスやリポジトリに接続できるように、ポート 443 経由の送信インターネット接続が必要です。"エンドポイントのリストを表示する" 。

NetApp Copy and Sync は、同期関係を作成するときにインストール プロセスをガイドします。その時点で、クラウドにデータ ブローカーを展開したり、独自の Linux ホスト用のインストール スクリプトをダウンロードしたりできます。

- "AWSのインストールを確認する"
- "Azureのインストールを確認する"
- "Google Cloud のインストールを確認する"
- "Linuxホストのインストールを確認する"

4 最初の同期関係を作成する

ログイン "NetApp Console"をクリックし、[同期] を選択して、ソースとターゲットの選択内容をドラッグ アンド ドロップします。指示に従ってセットアップを完了します。"詳細情報" 。

5 無料トライアル終了後は同期関係の料金をお支払いください

AWS または Azure から従量課金制または年間支払いでサブスクライブします。または、 NetAppから直接ライセンスを購入します。 NetApp Copy and Syncのライセンス設定ページに移動して設定するだけです。"詳細情報" 。

NetApp Copy and Syncでサポートされている同期関係

NetApp Copy and Sync を使用すると、ソースからターゲットにデータを同期できます。これを同期関係と呼びます。始める前に、サポートされている関係を理解しておく必要があります。

ソースの場所	サポートされているターゲットの場所
アマゾンEFS	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
Amazon FSx for ONTAP	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
Amazon S3	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • ボックス[1] • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure ブロブ	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
Azure データレイクストレージ Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • ONTAP向け FSx • IBM Cloud Object Storage • NFS サーバ • オンプレミスONTAP • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure NetApp Files	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
ボックス[1]	• Amazon FSx for ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM Cloud Object Storage • NFS サーバ • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
Cloud Volumes ONTAP	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
Google Cloud Storage	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Googleドライブ	• NFS サーバ • SMB サーバ

ソースの場所	サポートされているターゲットの場所
IBM Cloud Object Storage	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • ボックス[1] • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
NFS サーバ	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Googleドライブ • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
オンプレミスのONTAPクラスタ（NFS または SMB）	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
ONTAP S3 ストレージ	• Amazon S3 • Azure データレイクストレージ Gen2 • Google Cloud Storage • NFS サーバ • SMB サーバ • StorageGRID • ONTAP S3 ストレージ
SFTP [2]	S3

ソースの場所	サポートされているターゲットの場所
SMB サーバ	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Googleドライブ • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
StorageGRID	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • ボックス[1] • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID

注：

1. Box サポートはプレビューとして利用できます。

2. このソース/ターゲットとの同期関係は、コピーおよび同期 API の使用によってのみサポートされます。
3. BLOB コンテナーがターゲットの場合は、特定の Azure BLOB ストレージ層を選択できます。
    - ホットストレージ
    - クールストレージ
4. Amazon S3 がターゲットの場合は、特定の S3 ストレージクラスを選択できます。
    - 標準（これがデフォルトのクラスです）
    - インテリジェントティアリング
    - 標準-低頻度アクセス
    - 1つのゾーン - 低頻度アクセス
    - グレイシャーディープアーカイブ
    - 氷河フレキシブルリトリーバル
    - 氷河の即時検索
5. Google Cloud Storage バケットがターゲットの場合は、特定のストレージ クラスを選択できます。
    - Standard
    - ニアライン
    - コールドライン
    - アーカイブ

NetApp Copy and Syncでソースとターゲットを準備する

ソースとターゲットがNetApp Copy and Syncの次の要件を満たしていることを確認します。

ネットワーク

- ソースとターゲットは、データ ブローカー グループへのネットワーク接続を持っている必要があります。

  たとえば、NFS サーバーがデータセンターにあり、データブローカーが AWS にある場合は、ネットワークから VPC へのネットワーク接続 (VPN または Direct Connect) が必要です。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

ターゲット ディレクトリ

同期関係を作成するときに、「コピーと同期」を使用すると、既存のターゲット ディレクトリを選択し、必要に応じてそのディレクトリ内に新しいフォルダーを作成できます。したがって、優先するターゲット ディレクトリがすでに存在することを確認してください。

ディレクトリの読み取り権限

ソースまたはターゲット内のすべてのディレクトリまたはフォルダーを表示するには、コピーと同期にそのディレクトリまたはフォルダーに対する読み取り権限が必要です。

NFS

ファイルとディレクトリの uid/gid を使用して、ソース/ターゲット上で権限を定義する必要があります。

オブジェクト ストレージ

- AWS および Google Cloud の場合、データ ブローカーにはリスト オブジェクト権限が必要です (データ ブローカーのインストール手順に従うと、これらの権限はデフォルトで提供されます)。
- Azure、 StorageGRID、IBM の場合、同期関係を設定するときに入力する資格情報には、オブジェクトの一覧権限が必要です。

SMB

同期関係を設定するときに入力する SMB 資格情報には、リスト フォルダーのアクセス許可が必要です。

データブローカーは、デフォルトで次のディレクトリを無視します: .snapshot、~snapshot、.copy-offload

コピーと同期を使用して SMB データをCloud Volumes ONTAPにコピーする場合、ソース システムのファイルとフォルダーの所有権は保持されません。この動作は、コピーと同期が Linux SMB クライアントを使用し、転送の認証に使用されるユーザーまたはサービス アカウントに所有権を割り当てるために発生します。アクセス制御リストは保持される場合がありますが、所有権と監査情報はソース システムとは異なる場合があります。これは想定される動作です。

Amazon S3バケットの要件

Amazon S3 バケットが次の要件を満たしていることを確認してください。

Amazon S3 でサポートされているデータブローカーの場所

S3 ストレージを含む同期関係には、AWS またはオンプレミスにデプロイされたデータブローカーが必要です。どちらの場合でも、コピーと同期では、インストール中にデータブローカーを AWS アカウントに関連付けるように求められます。

- "AWSデータブローカーの導入方法を学ぶ"
- "Linuxホストにデータブローカーをインストールする方法を学ぶ"

サポートされている**AWS**リージョン

中国地域を除くすべての地域がサポートされています。

他の **AWS** アカウントの **S3** バケットに必要な権限

同期関係を設定するときに、データブローカーに関連付けられていない AWS アカウントにある S3 バケットを指定できます。

"このJSONファイルに含まれる権限"データ ブローカーがアクセスできるようにするには、その S3 バケット

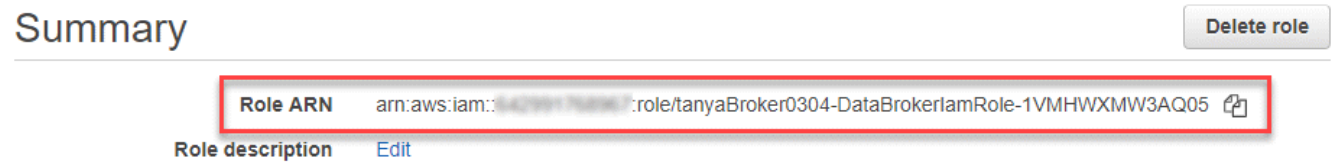
に適用する必要があります。これらの権限により、データ ブローカーはバケットとの間でデータをコピーしたり、バケット内のオブジェクトを一覧表示したりできるようになります。

JSON ファイルに含まれる権限については、次の点に注意してください。

1. *<BucketName>* は、データブローカーに関連付けられていない AWS アカウントにあるバケットの名前です。
2. *<RoleARN>* は、次のいずれかに置き換える必要があります。

   - データブローカーが Linux ホストに手動でインストールされた場合、*RoleARN* は、データブローカーのデプロイ時に AWS 認証情報を指定した AWS ユーザーの ARN である必要があります。
   - CloudFormation テンプレートを使用してデータブローカーが AWS にデプロイされた場合、*RoleARN* はテンプレートによって作成された IAM ロールの ARN である必要があります。

     ロール ARN を見つけるには、EC2 コンソールに移動し、データブローカーインスタンスを選択して、[説明] タブから IAM ロールを選択します。その後、IAM コンソールにロール ARN を含む概要ページが表示されます。



Azure Blobストレージの要件

Azure Blob ストレージが次の要件を満たしていることを確認してください。

Azure Blob でサポートされているデータ ブローカーの場所

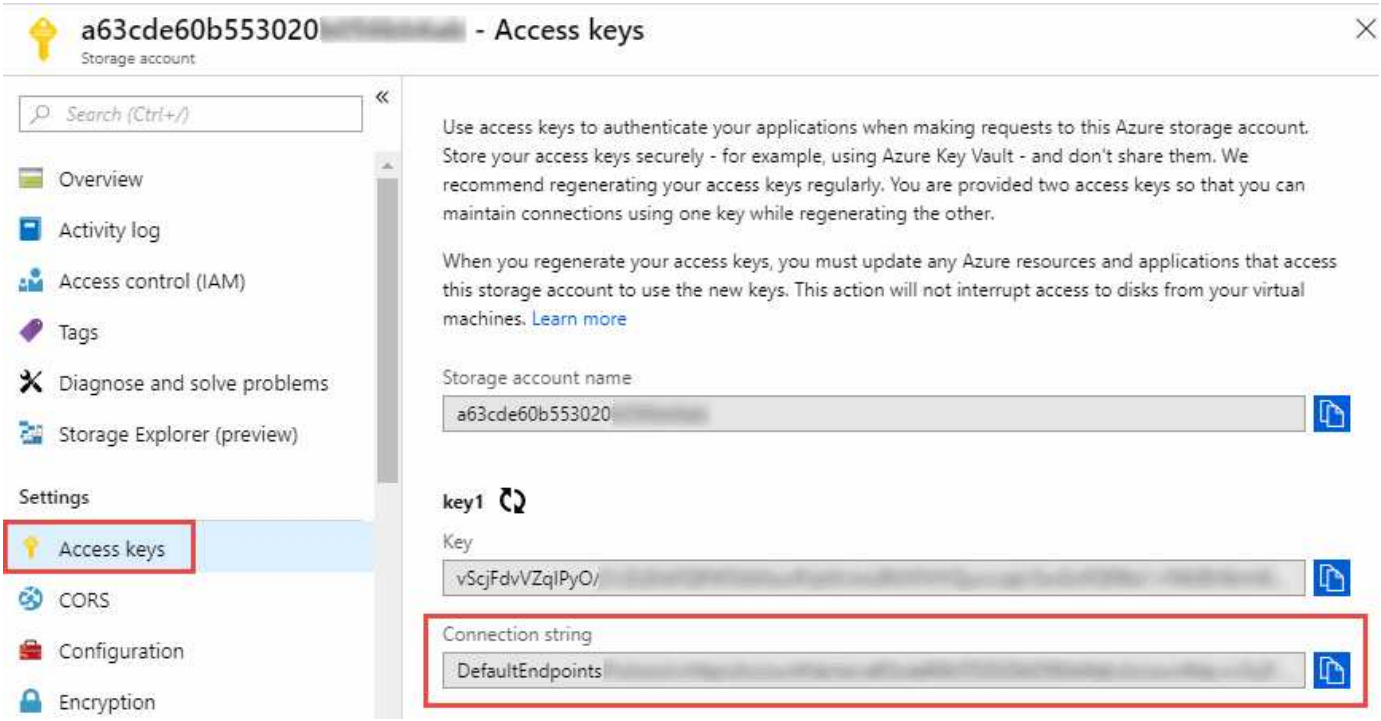
同期関係に Azure Blob Storage が含まれている場合、データ ブローカーは任意の場所に配置できます。

サポートされている**Azure**リージョン

中国、米国政府、米国国防総省地域を除くすべての地域がサポートされています。

Azure Blob と **NFS/SMB** を含む関係の接続文字列

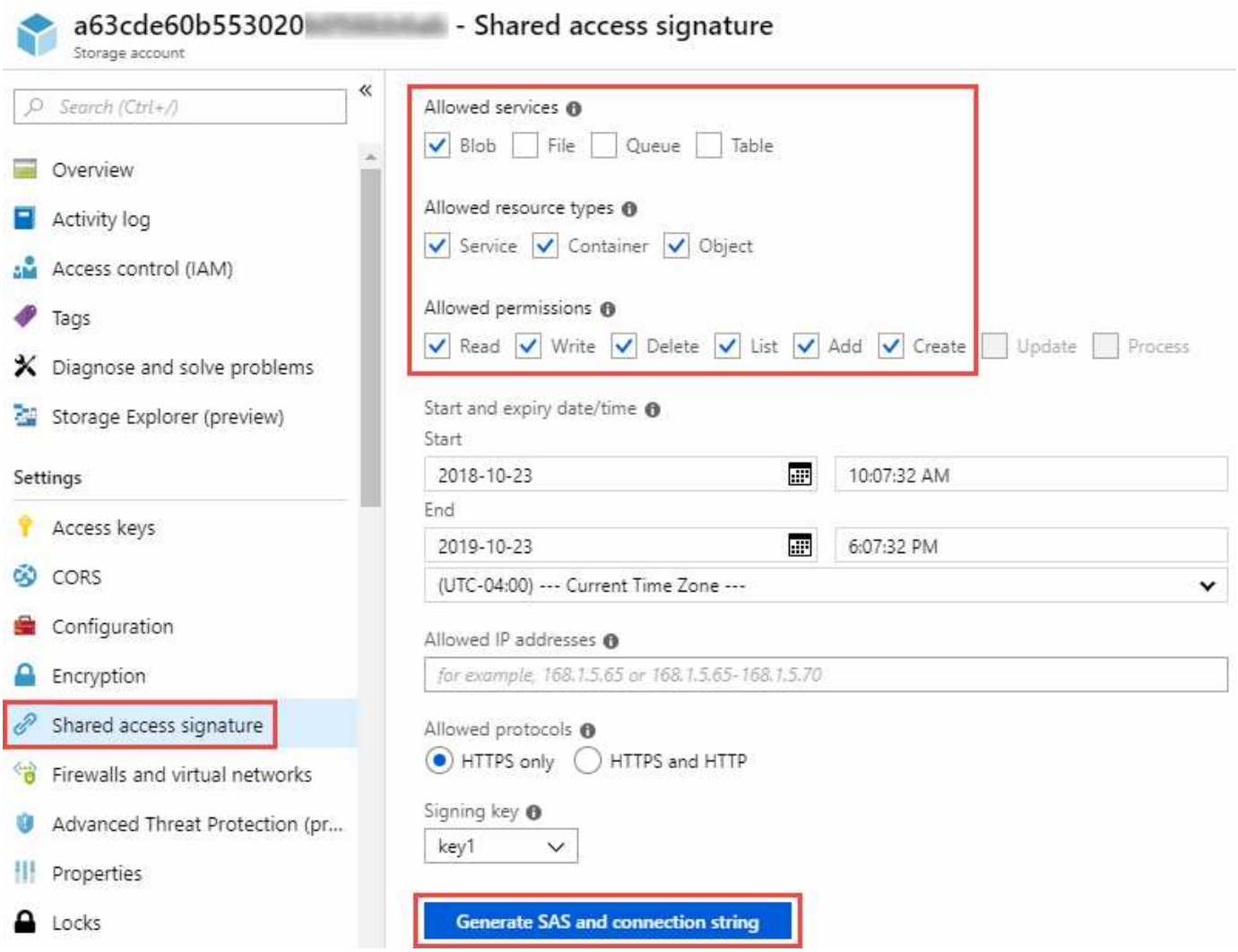
Azure BLOB コンテナーと NFS または SMB サーバー間の同期関係を作成するときは、Copy と Sync にストレージ アカウント接続文字列を指定する必要があります。



2つのAzure Blobコンテナ間でデータを同期したい場合は、接続文字列に "共有アクセス署名"（SAS）。また、Blob コンテナーと NFS または SMB サーバー間で同期するときに SAS を使用するオプションもあります。

SAS は、Blob サービスおよびすべてのリソース タイプ (サービス、コンテナー、オブジェクト) へのアクセスを許可する必要があります。 SAS には次の権限も含まれている必要があります。

- ソースBLOBコンテナの場合: 読み取りとリスト
- 対象のBLOBコンテナの場合: 読み取り、書き込み、一覧表示、追加、作成



を選択すると利用できます。"]

Azure BLOB コンテナーを含む継続的な同期関係を実装する場合は、通常の接続文字列または SAS 接続文字列を使用できます。 SAS 接続文字列を使用する場合は、近い将来に期限切れになるように設定しないでください。

Azure データレイクストレージ Gen2

Azure Data Lake を含む同期関係を作成する場合は、Copy and Sync にストレージ アカウント接続文字列を提供する必要があります。共有アクセス署名 (SAS) ではなく、通常の接続文字列である必要があります。

Azure NetApp Files の要件

Azure NetApp Filesとの間でデータを同期する場合は、Premium または Ultra サービス レベルを使用します。ディスク サービス レベルが標準の場合、障害やパフォーマンスの問題が発生する可能性があります。

適切なサービス レベルを決定する際にサポートが必要な場合は、ソリューション アーキテクトにご相談ください。ボリューム サイズとボリューム ティアによって、取得できるスループットが決まります。

"Azure NetApp Files のサービス レベルとスループットの詳細" 。

ボックスの要件

- Box を含む同期関係を作成するには、次の資格情報を提供する必要があります。
  - クライアントID
  - Client secret
  - 秘密鍵
  - 公開鍵ID
  - パスフレーズ
  - エンタープライズID
- Amazon S3 から Box への同期関係を作成する場合は、次の設定が 1 に設定されている統合構成を持つデータ ブローカー グループを使用する必要があります。
  - スキャナの同時実行
  - スキャナプロセス制限
  - 転送者の同時実行
  - 転送プロセス制限

  "データブローカーグループの統一された構成を定義する方法を学びます" 。

Google Cloud Storage バケットの要件

Google Cloud Storage バケットが次の要件を満たしていることを確認してください。

Google Cloud Storage でサポートされているデータ ブローカーの場所

Google Cloud Storage を含む同期関係には、Google Cloud またはオンプレミスにデプロイされたデータ ブローカーが必要です。コピーと同期では、同期関係を作成するときに、データ ブローカーのインストール プロセスをガイドします。

- "Google Cloud データブローカーの導入方法を学ぶ"
- "Linuxホストにデータブローカーをインストールする方法を学ぶ"

サポートされている Google Cloud リージョン

すべての地域がサポートされています。

他の Google Cloud プロジェクトのバケットに対する権限

同期関係を設定するときに、データブローカーのサービス アカウントに必要な権限を付与すると、異なるプロジェクトの Google Cloud バケットから選択できます。"サービスアカウントの設定方法を学ぶ" 。

SnapMirrorの宛先に対する権限

同期関係のソースがSnapMirror の宛先 (読み取り専用) である場合、ソースからターゲットにデータを同期するには、「読み取り/リスト」権限で十分です。

Google Cloud バケットの暗号化

ターゲットの Google Cloud バケットは、顧客管理の KMS キーまたはデフォルトの Google 管理キーを使用して暗号化できます。バケットにすでに KMS 暗号化が追加されている場合は、デフォルトの Google 管理の暗号化が上書きされます。

顧客管理KMSキーを追加するには、 "正しい権限"キーはバケットと同じリージョンに存在する必要があります。

Googleドライブ

Google ドライブを含む同期関係を設定する場合は、次の情報を提供する必要があります。

- データを同期するGoogleドライブの場所にアクセスできるユーザーのメールアドレス
- Google ドライブにアクセスする権限を持つ Google Cloud サービス アカウントのメールアドレス
- サービスアカウントの秘密鍵

サービス アカウントを設定するには、Google ドキュメントの指示に従ってください。

- "サービスアカウントと資格情報を作成する"
- "ドメイン全体の権限をサービス アカウントに委任する"

OAuth スコープ フィールドを編集するときは、次のスコープを入力します。

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

NFSサーバの要件

- NFS サーバーは、 NetAppシステムでも非NetAppシステムでもかまいません。
- ファイル サーバーは、データ ブローカー ホストが必要なポート経由でエクスポートにアクセスできるようにする必要があります。
  - 111 TCP/UDP
  - 2049 TCP/UDP
  - 5555 TCP/UDP
- NFS バージョン 3、4.0、4.1、4.2 がサポートされています。

  必要なバージョンをサーバー上で有効にする必要があります。
- ONTAPシステムから NFS データを同期する場合は、SVM の NFS エクスポート リストへのアクセスが有効になっていることを確認します (vserver nfs modify -vserver *svm_name* -showmount enabled)。

  ONTAP 9.2 以降では、showmount のデフォルト設定は *enabled* になっています。

ONTAPの要件

同期関係にCloud Volumes ONTAPまたはオンプレミスのONTAPクラスターが含まれており、NFSv4 以降を選択した場合は、 ONTAPシステムで NFSv4 ACL を有効にする必要があります。 ACL をコピーするにはこれが必要です。

ONTAP S3 ストレージ要件

同期関係を設定すると、 "ONTAP S3 ストレージ" 、以下の情報を提供する必要があります。

- ONTAP S3に接続されているLIFのIPアドレス
- ONTAPが使用するように設定されているアクセス キーと秘密キー

SMBサーバの要件

- SMB サーバーは、 NetAppシステムでも非NetAppシステムでもかまいません。
- SMB サーバーに対する権限を持つ資格情報をコピーおよび同期に提供する必要があります。
  - ソース SMB サーバーには、リストと読み取りの権限が必要です。

    バックアップ オペレーター グループのメンバーは、ソース SMB サーバーでサポートされます。
  - ターゲット SMB サーバーには、リスト、読み取り、および書き込みの権限が必要です。
- ファイル サーバーは、データ ブローカー ホストが必要なポート経由でエクスポートにアクセスできるようにする必要があります。
  - 139 TCP
  - 445 TCP
  - 137-138 UDP
- SMB バージョン 1.0、2.0、2.1、3.0、3.11 がサポートされています。
- 「Administrators」グループに、ソース フォルダーとターゲット フォルダーに対する「フル コントロール」権限を付与します。

  この権限を付与しないと、データ ブローカーにはファイルまたはディレクトリの ACL を取得するための十分な権限がない可能性があります。この問題が発生すると、次のエラーが表示されます: 「getxattr error 95」

隠しディレクトリとファイルに対する **SMB** 制限

SMB 制限は、SMB サーバー間でデータを同期するときに隠しディレクトリとファイルに影響します。ソース SMB サーバー上のディレクトリまたはファイルのいずれかが Windows によって非表示になっている場合、非表示属性はターゲット SMB サーバーにコピーされません。

大文字と小文字を区別しない制限による **SMB** 同期の動作

SMB プロトコルは大文字と小文字を区別しません。つまり、大文字と小文字は同じものとして扱われます。同期関係に SMB サーバーが含まれており、ターゲットにデータがすでに存在する場合、この動作によりファイルが上書きされ、ディレクトリのコピー エラーが発生する可能性があります。

たとえば、ソースに「a」という名前のファイルがあり、ターゲットに「A」という名前のファイルがあるとします。コピーと同期によって「a」という名前のファイルがターゲットにコピーされると、ファイル「A」はソースのファイル「a」によって上書きされます。

ディレクトリの場合、ソースに「b」という名前のディレクトリがあり、ターゲットに「B」という名前のディレクトリがあるとします。コピーと同期が「b」という名前のディレクトリをターゲットにコピーしようとすると、ディレクトリがすでに存在するというエラーがコピーと同期によって受信されます。その結果、コピーと同期では常に「b」という名前のディレクトリのコピーに失敗します。

この制限を回避する最善の方法は、データを空のディレクトリに同期することです。

NetApp Copy and Syncのネットワーク概要

NetApp Copy and Syncのネットワークには、データ ブローカー グループとソースおよびターゲットの場所間の接続、およびポート 443 経由のデータ ブローカーからの送信インターネット接続が含まれます。

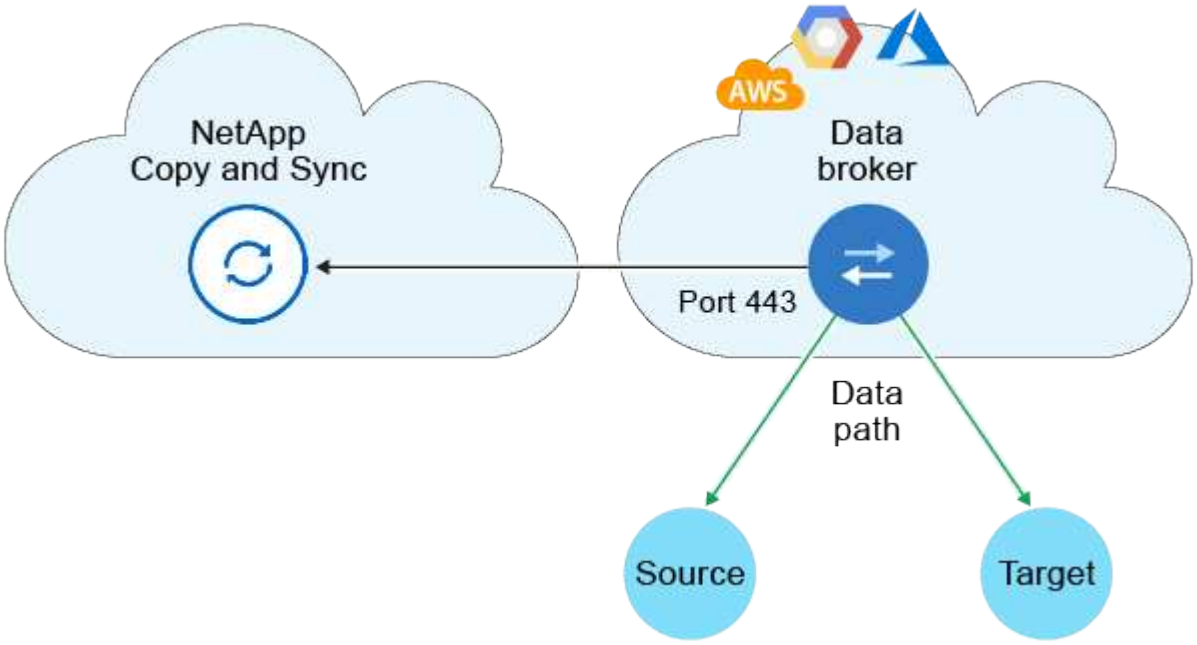
データブローカーの場所

データ ブローカー グループは、クラウドまたはオンプレミスにインストールされた 1 つ以上のデータ ブローカーで構成されます。

クラウド上のデータブローカー

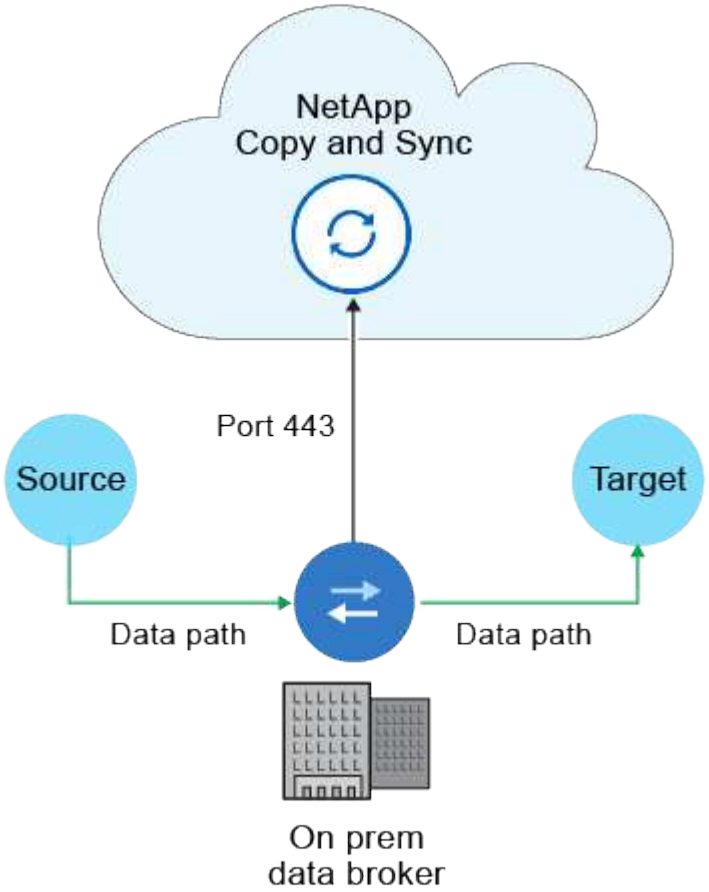
次の画像は、AWS、Google Cloud、または Azure のいずれかのクラウドで実行されているデータ ブローカーを示しています。データ ブローカーに接続している限り、ソースとターゲットは任意の場所に配置できます。たとえば、データセンターからクラウド プロバイダーへの VPN 接続がある場合があります。

Copy and Sync がデータ ブローカーを AWS、Azure、または Google Cloud にデプロイすると、必要な送信通信を有効にするセキュリティ グループが作成されます。



オンプレミスのデータブローカー

次の図は、データセンター内のオンプレミスで実行されているデータ ブローカーを示しています。繰り返しになりますが、データ ブローカーに接続されていれば、ソースとターゲットは任意の場所に配置できます。



ネットワーク要件

- ソースとターゲットは、データ ブローカー グループへのネットワーク接続を持っている必要があります。

  たとえば、NFS サーバーがデータセンターにあり、データブローカーが AWS にある場合は、ネットワークから VPC へのネットワーク接続 (VPN または Direct Connect) が必要です。

- データ ブローカーには、ポート 443 経由でタスクのコピーと同期をポーリングできるように、送信インターネット接続が必要です。
- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

ネットワークエンドポイント

NetAppデータ ブローカーでは、コピーおよび同期と通信し、他のいくつかのサービスやリポジトリに接続するために、ポート 443 経由の送信インターネット アクセスが必要です。ローカル Web ブラウザでも、特定のアクションのためにエンドポイントへのアクセスが必要です。送信接続を制限する必要がある場合は、送信トラフィック用にファイアウォールを構成するときに、次のエンドポイントのリストを参照してください。

データブローカーエンドポイント

データ ブローカーは次のエンドポイントに接続します。

エンドポイント	目的
https://olcentgbl.trafficmanager.net	データ ブローカー ホストの CentOS パッケージを更新するためのリポジトリに接続します。このエンドポイントは、CentOS ホストにデータ ブローカーを手動でインストールした場合にのみ接続されます。
https://rpm.nodesource.com https://registry.npmjs.org https://nodejs.org:	開発で使用される Node.js、npm、その他のサードパーティ パッケージを更新するためにリポジトリに問い合わせます。
https://tgz.pm2.io	コピーと同期を監視するために使用されるサードパーティ パッケージである PM2 を更新するためのリポジトリにアクセスします。
https://sqs.us-east-1.amazonaws.com https://kinesis.us-east-1.amazonaws.com	Copy and Sync が操作 (ファイルのキューイング、アクションの登録、データブローカーへの更新の配信) に使用する AWS サービスに接続します。
https://s3.*region*.amazonaws.com 例: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["S3エンドポイントのリストについてはAWSドキュメントを参照してください。"^]	同期関係に S3 バケットが含まれている場合に Amazon S3 に接続します。
https://s3.amazonaws.com/	Copy and Sync からデータ ブローカー ログをダウンロードすると、データ ブローカーはログ ディレクトリを zip ファイルに圧縮し、us-east-1 リージョンの定義済み S3 バケットにログをアップロードします。
https://storage.googleapis.com/	同期関係で GCP バケットが使用されるときに Google Cloud に接続します。
https://storage-account.blob.core.windows.netAzure Data Lake Gen2 を使用する場合:https://storage-account.dfs.core.windows.net[]ここで、storage-account はユーザーのソース ストレージ アカウントです。	ユーザーの Azure ストレージ アカウント アドレスへのプロキシを開きます。
https://cf.cloudsync.netapp.com https://repo.cloudsync.netapp.com	Copy and Sync に連絡するには。
https://support.netapp.com	同期関係に BYOL ライセンスを使用する場合は、 NetAppサポートにお問い合わせください。
https://fedoraproject.org	インストールおよび更新中にデータ ブローカー仮想マシンに 7z をインストールします。 AutoSupportメッセージをNetAppテクニカル サポートに送信するには、7z が必要です。

エンドポイント	目的
https://sts.amazonaws.com https://sts.us-east-1.amazonaws.com	データブローカーが AWS にデプロイされている場合、またはオンプレミスにデプロイされていて AWS 認証情報が提供されている場合に、AWS 認証情報を検証します。データ ブローカーは、デプロイ中、更新時、および再起動時にこのエンドポイントに接続します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com	分類を使用して新しい同期関係のソース ファイルを選択するときに、 NetApp Data Classificationに問い合わせます。
https://pubsub.googleapis.com	Google ストレージ アカウントから継続的な同期関係を作成する場合。
https://storage-account</ em>.queue.core.windows.net\https://management.azure.com/subscriptions/${subscriptionId} /resourceGroups/${resourceGroup}/providers/Microsoft.EventGrid/* ここで、storage-account はユーザーのソース ストレージ アカウント、subscriptionid はソース サブスクリプション ID 、resourceGroup はソース リソース グループです。	Azure ストレージ アカウントから継続的な同期関係を作成する場合。

Webブラウザのエンドポイント

トラブルシューティングのためにログをダウンロードするには、Web ブラウザが次のエンドポイントにアクセスできる必要があります。

ログ.cloudsync.netapp.com:443

NetApp Copy and Syncにログイン

NetApp Consoleを使用してNetApp Copy and Syncにログインします。

コンソールにログインするには、 NetAppサポート サイトの認証情報を使用するか、電子メールとパスワードを使用してNetAppクラウド ログインにサインアップすることができます。 "ログインについて詳しくはこちら" 。

NetApp Copy and Sync は、アイデンティティ アクセス管理を使用して、各ユーザーの特定のアクションへのアクセスを制御します。

必要な**NetApp Console**ロール 組織管理者ロール。 "NetApp Consoleのアクセスロールについて学ぶ" 。

手順

1. ウェブブラウザを開いて、 "NetApp Console" 。

   NetApp Consoleのログイン ページが表示されます。

2. コンソールにログインします。
3. コンソールの左側のナビゲーションから、モビリティ > *コピーと同期*を選択します。

データブローカーをインストールする

NetApp Copy and Sync用の新しいデータブローカーを AWS に作成する

NetApp Copy and Syncの新しいデータ ブローカー グループを作成するときは、Amazon Web Services を選択して、VPC 内の新しい EC2 インスタンスにデータ ブローカー ソフトウェアをデプロイします。 NetApp Copy and Sync はインストール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

クラウド内またはオンプレミスの既存の Linux ホストにデータ ブローカーをインストールすることもできます。"詳細情報" 。

サポートされているAWSリージョン

中国地域を除くすべての地域がサポートされています。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、root として実行する必要があります。たとえば、共有をマウントします。

ネットワーク要件

- データ ブローカーには、ポート 443 経由でタスクのコピーと同期をポーリングできるように、送信インターネット接続が必要です。

  Copy and Sync が AWS にデータブローカーをデプロイすると、必要なアウトバウンド通信を有効にするセキュリティグループが作成されます。インストール プロセス中にプロキシ サーバーを使用するようにデータ ブローカーを構成できることに注意してください。

  アウトバウンド接続を制限する必要がある場合は、"データブローカーが接続するエンドポイントのリスト" 。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

AWS にデータブローカーをデプロイするために必要な権限

データブローカーをデプロイするために使用するAWSユーザーアカウントには、次の権限が必要です。"NetAppが提供するこのポリシー" 。

AWSデータブローカーで独自のIAMロールを使用するための要件

Copy and Sync がデータ ブローカーをデプロイすると、データ ブローカー インスタンスの IAM ロールが作

成されます。必要に応じて、独自の IAM ロールを使用してデータ ブローカーをデプロイすることもできます。組織に厳格なセキュリティ ポリシーがある場合は、このオプションを使用することをお勧めします。

IAM ロールは次の要件を満たしている必要があります。

- EC2 サービスには、信頼できるエンティティとして IAM ロールを引き受ける権限が必要です。
- "このJSONファイルで定義された権限"データブローカーが適切に機能するには、IAM ロールに添付する必要があります。

データブローカーをデプロイするときに IAM ロールを指定するには、以下の手順に従います。

データブローカーを作成する

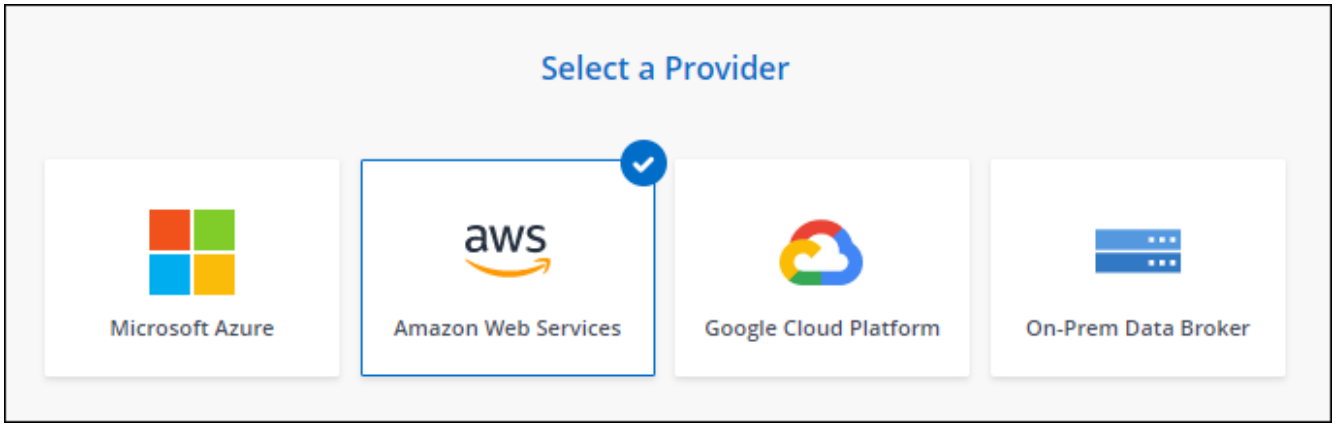
新しいデータ ブローカーを作成するには、いくつかの方法があります。これらの手順では、同期関係を作成するときに AWS にデータブローカーをインストールする方法について説明します。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *同期関係の定義*ページで、ソースとターゲットを選択し、*続行*を選択します。

   データ ブローカー グループ ページに到達するまで手順を完了します。

4. データ ブローカー グループ ページで、データ ブローカーの作成 を選択し、**Amazon Web Services** を選択します。



5. データ ブローカーの名前を入力し、[続行] を選選択します。
6. AWS アクセスキーを入力すると、Copy and Sync がユーザーに代わって AWS にデータブローカーを作成できるようになります。

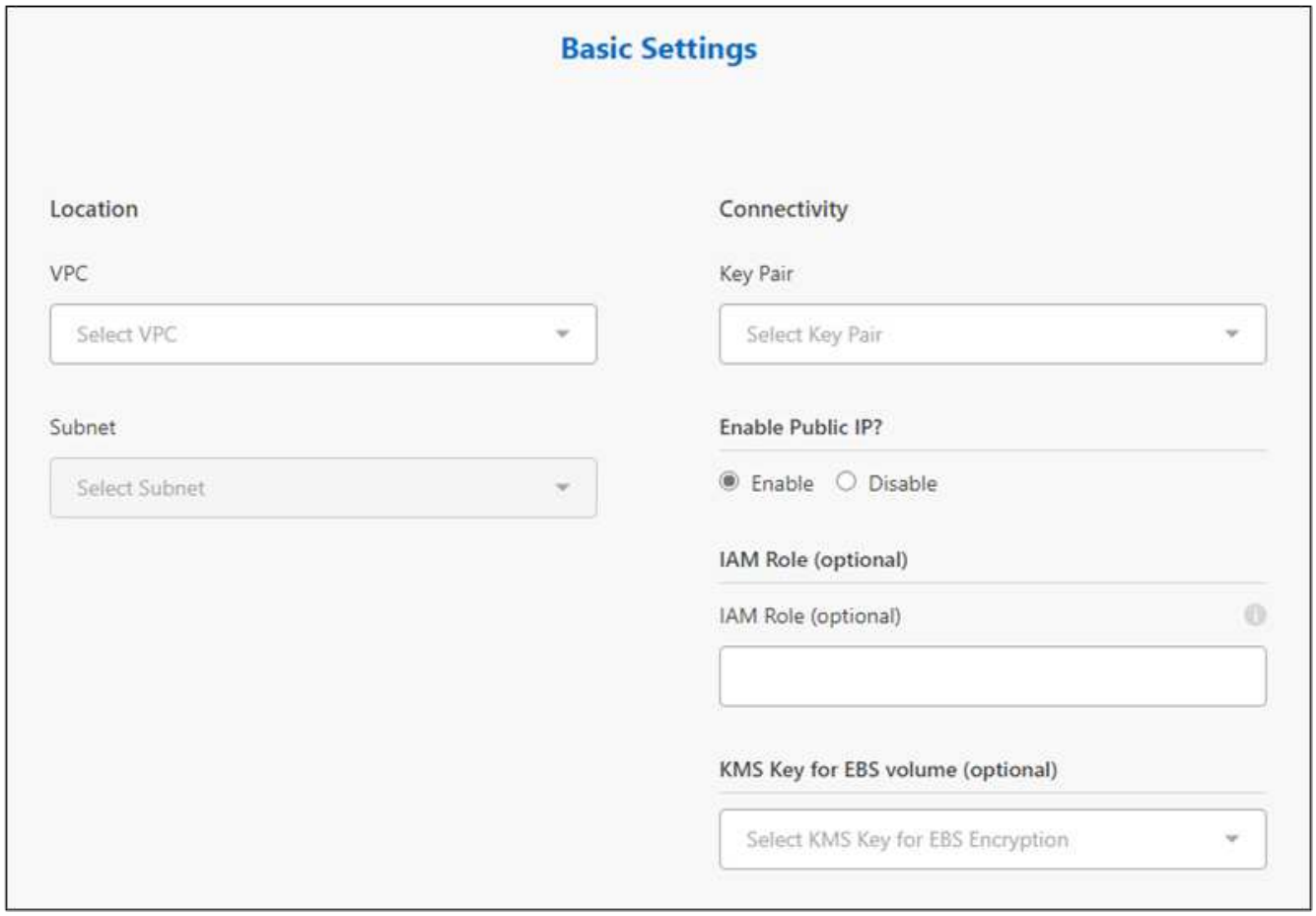
   キーは保存されず、他の目的にも使用されません。

   アクセス キーを提供したくない場合は、ページの下部にあるリンクを選択して、代わりに CloudFormation テンプレートを使用します。このオプションを使用する場合は、AWS に直接ログインするため、認証情報を提供する必要はありません。

   次のビデオでは、CloudFormation テンプレートを使用してデータブローカーインスタンスを起動する方法を示します。

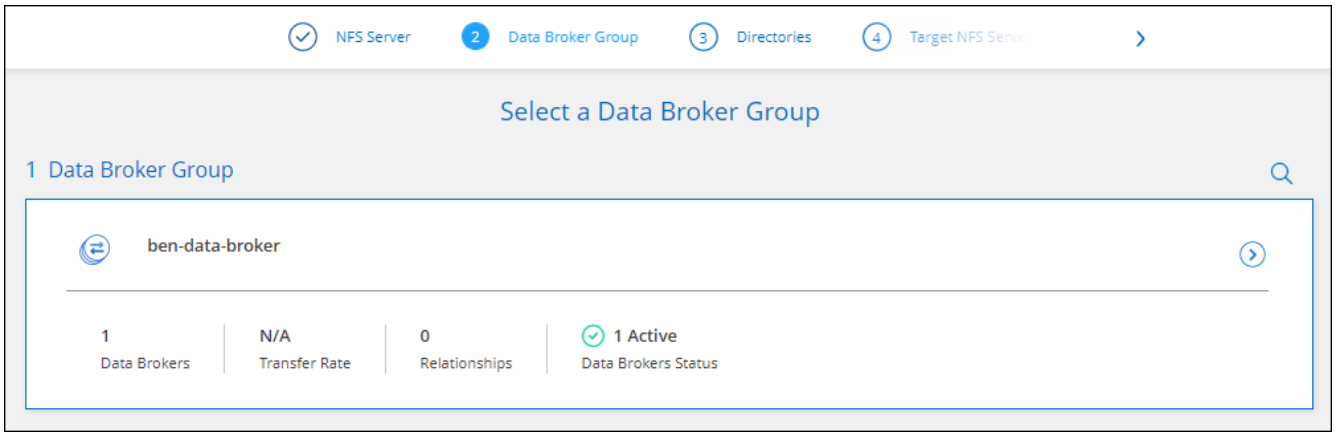
7. AWS アクセスキーを入力した場合は、インスタンスの場所を選択し、キーペアを選択し、パブリック IP アドレスを有効にするかどうかを選択し、既存の IAM ロールを選択するか、フィールドを空白のままにして、コピーと同期によってロールが自動的に作成されるようにします。 KMS キーを使用してデータ ブローカーを暗号化するオプションもあります。

   独自のIAMロールを選択した場合は、必要な権限を与える必要があります 。



8. VPC でのインターネット アクセスにプロキシが必要な場合は、プロキシ設定を指定します。
9. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。

   次の画像は、AWS に正常にデプロイされたインスタンスを示しています。



10. ウィザードのページを完了して、新しい同期関係を作成します。

結果

AWS にデータブローカーをデプロイし、新しい同期関係を作成しました。このデータ ブローカー グループを追加の同期関係で使用できます。

データブローカーインスタンスの詳細

コピーと同期は、次の構成を使用して AWS にデータブローカーを作成します。

Node.js の互換性
: バージョン21.2.0

インスタンスタイプ
: リージョンで利用可能な場合は m5n.xlarge、そうでない場合は m5.xlarge

vCPU
: 4

RAM
: 16 GB

オペレーティング システム
: Amazon Linux 2023

ディスクのサイズと種類
: 10 GB GP2 SSD

Azure でNetApp Copy and Sync用の新しいデータ ブローカーを作成する

NetApp Copy and Syncの新しいデータ ブローカー グループを作成するときは、Microsoft Azure を選択して、VNet 内の新しい仮想マシンにデータ ブローカー ソフトウェアを展開します。 NetApp Copy and Sync はインストール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

クラウド内またはオンプレミスの既存の Linux ホストにデータ ブローカーをインストールすることもできま

す。"詳細情報" 。

サポートされている**Azure**リージョン

中国、米国政府、米国国防総省地域を除くすべての地域がサポートされています。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、root として実行する必要があります。たとえば、共有をマウントします。

ネットワーク要件

- データ ブローカーには、ポート 443 経由でタスクのコピーおよび同期サービスをポーリングできるように、送信インターネット接続が必要です。

  コピーと同期によって Azure にデータ ブローカーがデプロイされると、必要な送信通信を有効にするセキュリティ グループが作成されます。

  アウトバウンド接続を制限する必要がある場合は、"データブローカーが接続するエンドポイントのリスト" 。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

Azure にデータ ブローカーをデプロイするために必要な権限

データ ブローカーをデプロイするために使用する Azure ユーザー アカウントに次のアクセス許可があることを確認します。

```
{
    "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/agreements/write"

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

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

注：

1. 以下の権限は、 "連続同期設定" Azure から別のクラウド ストレージの場所への同期関係について:
    - '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/アクション',
    - 'Microsoft.EventGrid/systemTopics/read'、
    - 'Microsoft.EventGrid/systemTopics/write',
    - 'Microsoft.EventGrid/systemTopics/削除',
    - 'Microsoft.EventGrid/eventSubscriptions/write',
    - 'Microsoft.Storage/storageAccounts/write'

    さらに、Azure で継続的な同期を実装する予定の場合は、割り当て可能なスコープをリソース グループ スコープではなくサブスクリプション スコープに設定する必要があります。
2. 次の権限は、データ ブローカーの作成に独自のセキュリティを選択する場合にのみ必要です。
    - 「Microsoft.Network/ネットワークセキュリティグループ/セキュリティルール/読み取り」
    - 「Microsoft.Network/networkSecurityGroups/読み取り」

認証方式

データ ブローカーをデプロイするときに、仮想マシンの認証方法 (パスワードまたは SSH 公開キーと秘密キーのペア) を選択する必要があります。

キーペアの作成方法については、以下を参照してください。 "Azure ドキュメント: Azure の Linux VM 用の SSH 公開キーと秘密キーのペアを作成して使用する" 。

データブローカーを作成する

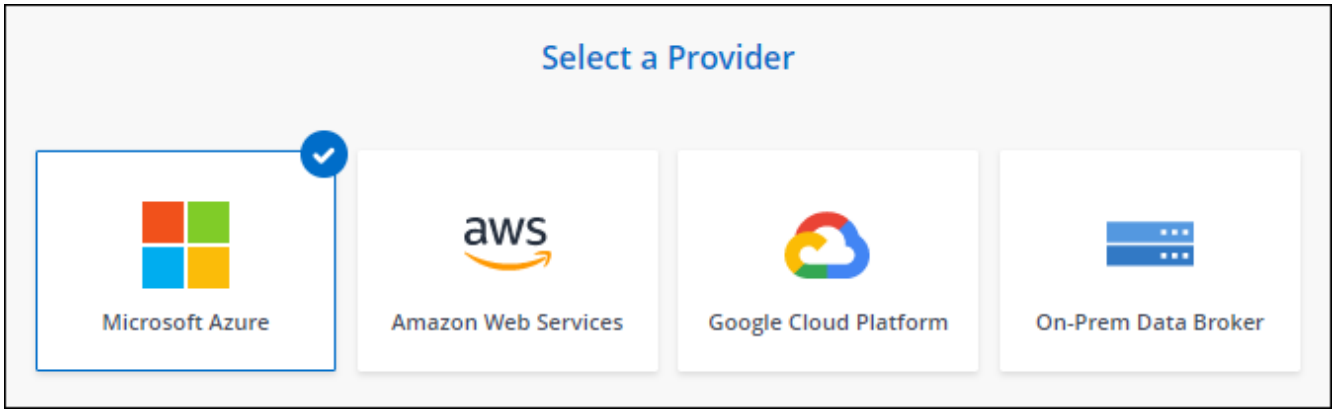
新しいデータ ブローカーを作成するには、いくつかの方法があります。次の手順では、同期関係を作成するときに Azure にデータ ブローカーをインストールする方法について説明します。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *同期関係の定義*ページで、ソースとターゲットを選択し、*続行*を選択します。

   データ ブローカー グループ ページに到達するまで手順を完了します。

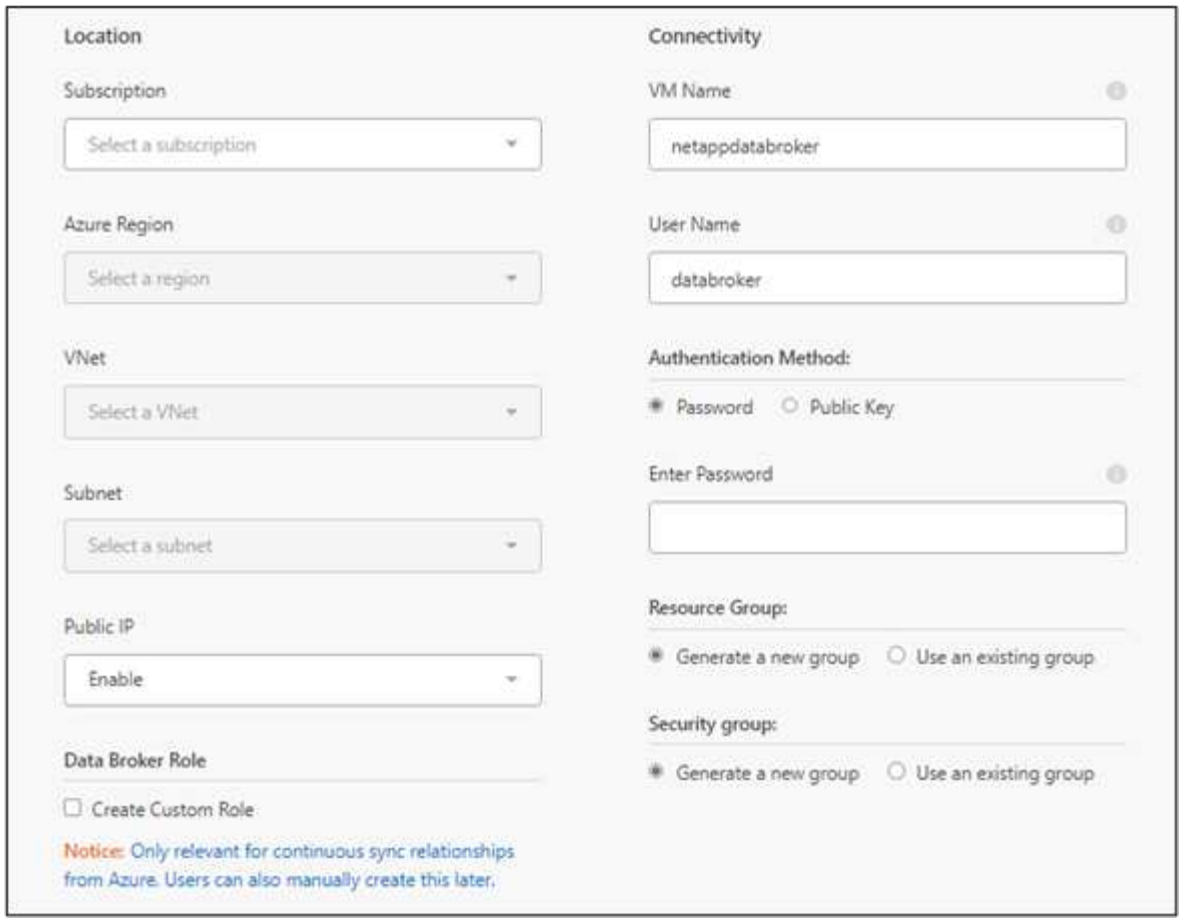
4. データ ブローカー グループ ページで、データ ブローカーの作成 を選択し、**Microsoft Azure** を選択します。



5. データ ブローカーの名前を入力し、[続行] を選択します。
6. プロンプトが表示されたら、Microsoft アカウントにログインします。プロンプトが表示されない場合は、[Azure にログイン] を選択します。

   このフォームは Microsoft によって所有およびホストされています。資格情報がNetAppに提供されていません。

7. データ ブローカーの場所を選択し、仮想マシンに関する基本的な詳細を入力します。



継続的な同期関係を実装する予定の場合は、データ ブローカーにカスタム ロールを割り当てる必要があります。これは、ブローカーの作成後に手動で行うこともできます。

8. VNet でのインターネット アクセスにプロキシが必要な場合は、プロキシ構成を指定します。
9. *続行*を選択します。データブローカーに S3 権限を追加する場合は、AWS アクセスキーとシークレットキーを入力します。
10. *続行*を選択し、デプロイメントが完了するまでページを開いたままにします。

    この処理には最大 7 分かかる場合があります。

11. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。
12. ウィザードのページを完了して、新しい同期関係を作成します。

結果

Azure にデータ ブローカーをデプロイし、新しい同期関係を作成しました。このデータ ブローカーは追加の同期関係で使用できます。

管理者の同意が必要であるというメッセージが表示されていますか?

コピーと同期にはユーザーに代わって組織内のリソースにアクセスする権限が必要であるため、管理者の承認が必要であると Microsoft から通知された場合は、次の 2 つのオプションがあります。

1. AD 管理者に次の権限を付与するよう依頼してください。

   Azure で、管理センター **> Azure AD >** ユーザーとグループ **>** ユーザー設定 に移動し、ユーザーはアプリが自分に代わって会社のデータにアクセスすることに同意できます を有効にします。

2. 次の URL (管理者の同意エンドポイント) を使用して、AD 管理者に代わって **CloudSync-AzureDataBrokerCreator** に同意するよう依頼します。

   https://login.microsoftonline.com/{テナントIDを入力してください}/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

   URLに示されているように、アプリのURLは\https://cloudsync.netapp.comで、アプリケーションクライアントIDは8ee4ca3a-bafa-4831-97cc-5a38923cab85です。

データブローカー**VM**の詳細

コピーと同期は、次の構成を使用して Azure にデータ ブローカーを作成します。

Node.js の互換性
: バージョン21.2.0

VMタイプ
: 標準 DS4 v2

vCPU
: 8

RAM
: 28 GB

オペレーティング システム
: ロッキーLinux 9.0

ディスクのサイズと種類
: 64 GB プレミアム SSD

Google Cloud で**NetApp Copy and Sync**用の新しいデータ ブローカーを作成する

NetApp Copy and Syncの新しいデータ ブローカー グループを作成するときは、Google Cloud Platform を選択して、Google Cloud VPC 内の新しい仮想マシン インスタンスにデータ ブローカー ソフトウェアをデプロイします。 NetApp Copy and Sync はインスト

ール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

クラウド内またはオンプレミスの既存の Linux ホストにデータ ブローカーをインストールすることもできます。"詳細情報" 。

サポートされている **Google Cloud** リージョン

すべての地域がサポートされています。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、root として実行する必要があります。たとえば、共有をマウントします。

ネットワーク要件

- データ ブローカーには、ポート 443 経由でタスクのコピーと同期をポーリングできるように、送信インターネット接続が必要です。

  Copy and Sync が Google Cloud にデータ ブローカーをデプロイすると、必要な送信通信を有効にするセキュリティ グループが作成されます。

  アウトバウンド接続を制限する必要がある場合は、"データブローカーが接続するエンドポイントのリスト" 。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

Google Cloud にデータブローカーをデプロイするために必要な権限

データ ブローカーをデプロイする Google Cloud ユーザーに次の権限があることを確認します。

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

サービスアカウントに必要な権限

データ ブローカーをデプロイするときは、次の権限を持つサービス アカウントを選択する必要があります。

```
- 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
```

注：

1. 「iam.serviceAccounts.signJwt」権限は、外部の HashiCorp ボールトを使用するようにデータ ブローカーを設定する場合にのみ必要です。
2. 「pubsub.*」および「storage.buckets.update」権限は、Google Cloud Storage から別のクラウド ストレージの場所への同期関係で継続的な同期設定を有効にする場合にのみ必要です。"継続同期オプションの詳細" 。
3. 「cloudkms.cryptoKeys.list」および「cloudkms.keyRings.list」権限は、ターゲットの Google Cloud Storage バケットで顧客管理の KMS キーを使用する予定の場合にのみ必要です。

データブローカーを作成する

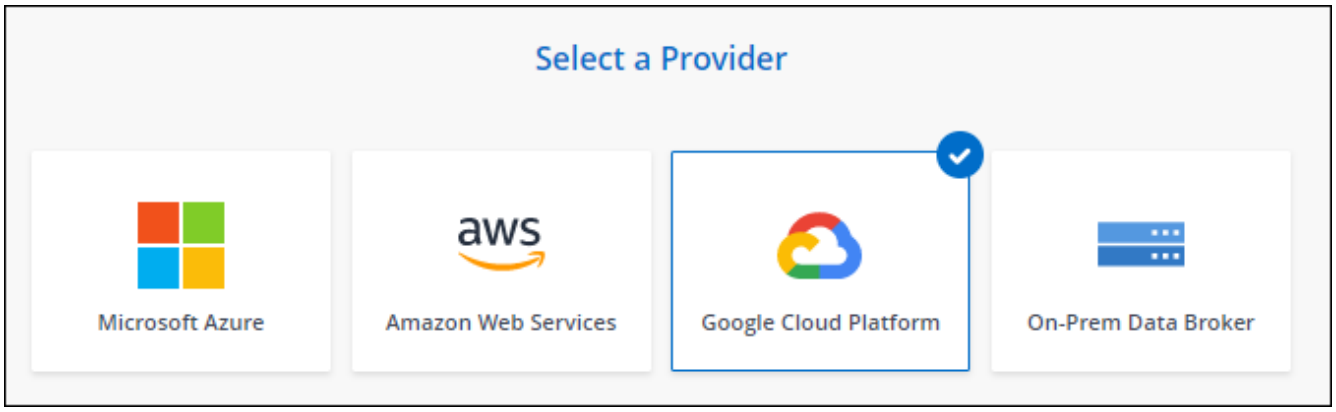
新しいデータ ブローカーを作成するには、いくつかの方法があります。次の手順では、同期関係を作成するときに Google Cloud にデータ ブローカーをインストールする方法について説明します。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *同期関係の定義*ページで、ソースとターゲットを選択し、*続行*を選択します。

データ ブローカー グループ ページに到達するまで手順を完了します。

4. データ ブローカー グループ ページで、データ ブローカーの作成 を選択し、**Google Cloud Platform** を選択します。

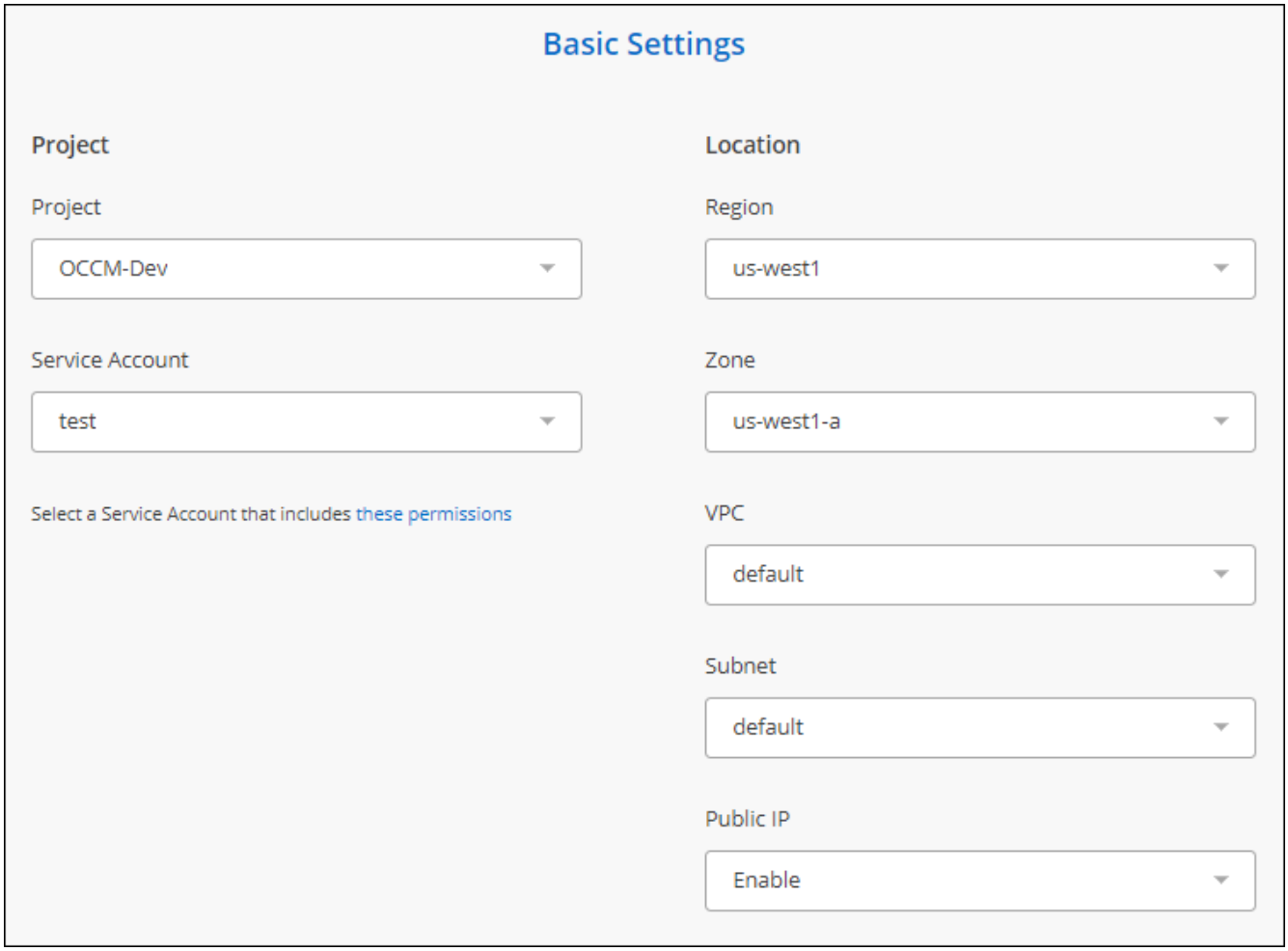


5. データ ブローカーの名前を入力し、[続行] を選択します。
6. プロンプトが表示されたら、Google アカウントでログインします。

   このフォームは Google が所有し、ホストしています。資格情報がNetAppに提供されていません。

7. プロジェクトとサービス アカウントを選択し、データ ブローカーの場所を選択します (パブリック IP アドレスを有効にするか無効にするかを含む)。

   パブリック IP アドレスを有効にしない場合は、次の手順でプロキシ サーバーを定義する必要があります。



8. VPC でのインターネット アクセスにプロキシが必要な場合は、プロキシ設定を指定します。

   インターネット アクセスにプロキシが必要な場合は、プロキシを Google Cloud 内に配置して、データ ブローカーと同じサービス アカウントを使用する必要があります。

9. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。

   インスタンスのデプロイには約 5 ～ 10 分かかります。コピーと同期の進行状況を監視できます。インスタンスが利用可能になると、自動的に更新されます。

10. ウィザードのページを完了して、新しい同期関係を作成します。

結果

Google Cloud にデータ ブローカーをデプロイし、新しい同期関係を作成しました。このデータ ブローカーは追加の同期関係で使用できます。

他の **Google Cloud** プロジェクトでバケットを使用する権限を付与する

同期関係を作成し、ソースまたはターゲットとして Google Cloud Storage を選択すると、コピーと同期により、データブローカーのサービス アカウントが使用権限を持つバケットから選択できるようになります。デフォルトでは、データ ブローカー サービス アカウントと同じプロジェクトにあるバケットが含まれます。ただし、必要な権限を付与すれば、他のプロジェクトからバケットを選択できます。

手順

1. Google Cloud Platform コンソールを開き、Cloud Storage サービスを読み込みます。
2. 同期関係のソースまたはターゲットとして使用するバケットの名前を選択します。
3. *権限*を選択します。
4. *追加*を選択します。
5. データ ブローカーのサービス アカウントの名前を入力します。
6. 提供する役割を選択してください上記と同じ権限。
7. *保存*を選択します。

結果

同期関係を設定するときに、そのバケットを同期関係のソースまたはターゲットとして選択できるようになりました。

データブローカー**VM**インスタンスの詳細

コピーと同期は、次の構成を使用して Google Cloud にデータ ブローカーを作成します。

Node.js の互換性
: バージョン21.2.0

機械の種類
: n2-標準-4

vCPU
: 4

RAM
: 15 GB

オペレーティング システム
: ロッキーLinux 9.0

ディスクのサイズと種類
: 20 GB HDD PD標準

NetApp Copy and Sync用のデータ ブローカーを **Linux** ホストにインストールします。

NetApp Copy and Syncの新しいデータ ブローカー グループを作成する場合は、オンプレミス データ ブローカー オプションを選択して、オンプレミスの Linux ホストまたはクラウド内の既存の Linux ホストにデータ ブローカー ソフトウェアをインストールします。 NetApp Copy and Sync はインストール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

Linuxホストの要件

- **Node.js** 互換性: v21.2.0

- オペレーティング･システム：
  - CentOS 8.0 および 8.5

    CentOS Streamはサポートされていません。
  - Red Hat Enterprise Linux 8.5、8.8、8.9、および 9.4
  - ロッキーLinux 9
  - Ubuntu Server 20.04 LTS、23.04 LTS、および 24.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    コマンド `yum update`データ ブローカーをインストールする前に、ホスト上で実行する必要があります。

  Red Hat Enterprise Linux システムは、Red Hat Subscription Management に登録する必要があります。登録されていない場合、システムはインストール中に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。
- **RAM**: 16 GB
- **CPU**: 4コア
- 空きディスク容量: 10 GB
- **SELinux**: ホスト上で SELinux を無効にすることをお勧めします。

  SELinux は、データ ブローカー ソフトウェアの更新をブロックするポリシーを適用し、通常の操作に必要なエンドポイントへのデータ ブローカーの接続をブロックできます。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、root として実行する必要があります。たとえば、共有をマウントします。

ネットワーク要件

- Linux ホストはソースとターゲットに接続されている必要があります。
- ファイル サーバーは、Linux ホストがエクスポートにアクセスできるようにする必要があります。
- AWS への送信トラフィック用に、Linux ホストでポート 443 が開いている必要があります (データブローカーは Amazon SQS サービスと常に通信します)。
- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

AWSへのアクセスを有効にする

S3 バケットを含む同期関係でデータ ブローカーを使用する予定の場合は、AWS アクセス用に Linux ホストを準備する必要があります。データブローカーをインストールするときは、プログラムによるアクセスと特定の権限を持つ AWS ユーザーに AWS キーを提供する必要があります。

手順

1. IAMポリシーを作成する "NetAppが提供するこのポリシー"

   "AWS の手順を見る"

2. プログラムによるアクセス権を持つ IAM ユーザーを作成します。

   "AWS の手順を見る"

   データブローカーソフトウェアをインストールするときに AWS キーを指定する必要があるので、必ずコピーしてください。

Google Cloudへのアクセスを有効にする

Google Cloud Storage バケットを含む同期関係でデータ ブローカーを使用する予定の場合は、Google Cloud アクセス用に Linux ホストを準備する必要があります。データ ブローカーをインストールするときは、特定の権限を持つサービス アカウントのキーを指定する必要があります。

手順

1. ストレージ管理者権限を持つ Google Cloud サービス アカウントをまだお持ちでない場合は作成します。
2. JSON 形式で保存されたサービス アカウント キーを作成します。

   "Google Cloud の手順を見る"

   ファイルには少なくとも次のプロパティが含まれている必要があります: "project_id"、"private_key"、および "client_email"

   キーを作成すると、ファイルが生成され、マシンにダウンロードされます。

3. JSON ファイルを Linux ホストに保存します。

Microsoft Azureへのアクセスを有効にする

Azure へのアクセスは、同期関係ウィザードでストレージ アカウントと接続文字列を指定することにより、関係ごとに定義されます。

データブローカーをインストールする

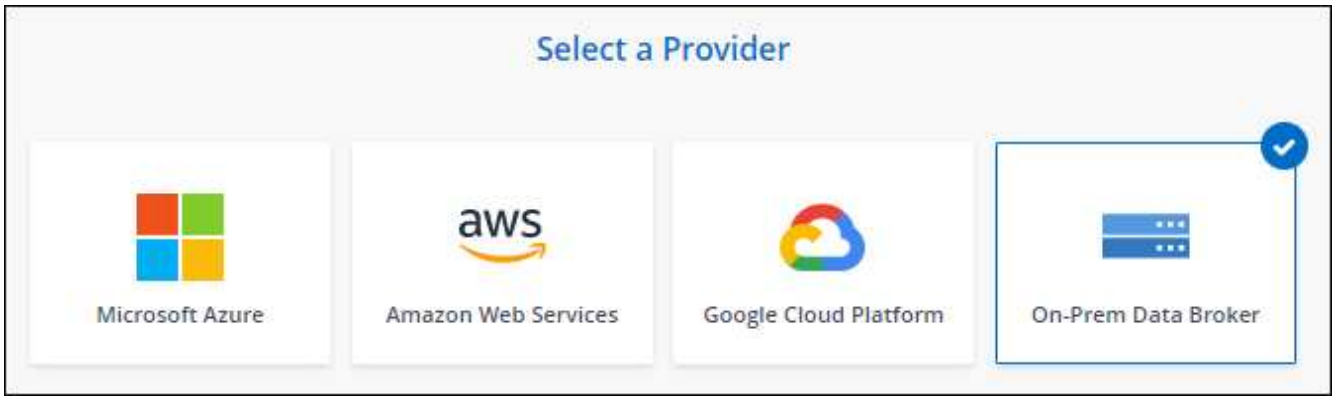
同期関係を作成するときに、Linux ホストにデータ ブローカーをインストールできます。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *同期関係の定義*ページで、ソースとターゲットを選択し、*続行*を選択します。

   データ ブローカー グループ ページに到達するまで手順を完了します。

4. データ ブローカー グループ ページで、データ ブローカーの作成 を選択し、オンプレミス データ ブローカー を選択します。



このオプションには ***On-Prem*** **Data Broker** というラベルが付いていますが、オンプレミスまたはクラウド内の Linux ホストに適用されます。

5. データ ブローカーの名前を入力し、[続行] を選択します。

   説明ページがすぐに読み込まれます。以下の手順に従う必要があります。手順にはインストーラーをダウンロードするための固有のリンクが含まれています。

6. 説明ページで：

   a. **AWS**、**Google Cloud**、またはその両方へのアクセスを有効にするかどうかを選択します。

   b. インストール オプションを選択します: プロキシなし、プロキシ サーバーを使用する、または 認証付きプロキシ サーバーを使用する。

      ユーザーはローカル ユーザーである必要があります。ドメイン ユーザーはサポートされていません。

   c. コマンドを使用して、データ ブローカーをダウンロードしてインストールします。

      次の手順では、可能な各インストール オプションの詳細について説明します。インストール オプションに基づいて正確なコマンドを取得するには、指示ページに従ってください。

   d. インストーラーをダウンロードしてください:

      - プロキシなし:

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

      - プロキシサーバーを使用する:

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

      - 認証付きプロキシサーバーを使用する:

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

        URI

        「コピーと同期」では、指示ページにインストール ファイルの URI が表示されます。この URI は、プロンプトに従ってオンプレミス データ ブローカーを展開すると読み込まれます。

リンクは動的に生成され、一度しか使用できないため、この URI はここでは繰り返されません。コピーと同期からURIを取得するには、次の手順に従います。 。

e. スーパーユーザーに切り替え、インストーラーを実行可能にしてソフトウェアをインストールします。

> 以下にリストされている各コマンドには、AWS アクセスと Google Cloud アクセスのパラメータが含まれています。インストール オプションに基づいて正確なコマンドを取得するには、指示ページに従ってください。

- プロキシ設定なし:

```
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>
```

- プロキシ設定:

```
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>
```

- 認証付きプロキシ構成:

```
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キー

これらは、ユーザーが準備しておくべきキーです以下の手順に従ってください。 AWS キーは、オンプレミスまたはクラウド ネットワークで実行されるデータ ブローカーに保存されます。 NetApp はデータ ブローカーの外部ではキーを使用しません。

JSONファイル

これは、準備しておくべきサービスアカウントキーを含むJSONファイルです。以下の手順に従ってください 。

7. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。
8. ウィザードのページを完了して、新しい同期関係を作成します。

NetApp Copy and Syncを使用する

ソースとターゲット間でデータを同期する

NetApp Copy and Syncのオブジェクト ストレージ間でデータを同期するためのデータ ブローカーを準備します。

NetApp Copy and Syncでオブジェクト ストレージからオブジェクト ストレージへ (たとえば、Amazon S3 から Azure Blob) データを同期する予定の場合は、同期関係を作成する前にデータ ブローカー グループを準備する必要があります。

タスク概要

データ ブローカー グループを準備するには、スキャナーの構成を変更する必要があります。構成を変更しないと、この同期関係でパフォーマンスの問題が発生する可能性があります。

開始する前に

オブジェクト ストレージからオブジェクト ストレージにデータを同期するために使用するデータ ブローカー グループは、これらのタイプの同期関係のみを管理する必要があります。データ ブローカー グループが異なるタイプの同期関係 (たとえば、NFS から NFS、またはオブジェクト ストレージから SMB) を管理している場合、それらの同期関係のパフォーマンスに悪影響が及ぶ可能性があります。

手順

1. "コピーと同期にログイン" 。
2. [コピーと同期] から、[データ ブローカーの管理] を選択します。
3. 選択
4. スキャナーの設定を更新します。
   a. *スキャナーの同時実行性*を*1*に変更します。
   b. *スキャナープロセスの制限*を*1*に変更します。
5. *構成の統合*を選択します。

結果

コピーと同期により、データ ブローカー グループの構成が更新されます。

次の手順

これで、構成したデータ ブローカー グループを使用して、オブジェクト ストレージ間の同期関係を作成できるようになりました。

NetApp Copy and Syncで同期関係を作成する

同期関係を作成すると、 NetApp Copy and Syncソースからターゲットにファイルがコピーされます。最初のコピーの後、コピーと同期は変更されたデータを 24 時間ごとに同期します。

一部のタイプの同期関係を作成するには、まずNetApp Consoleでシステムを作成する必要があります。

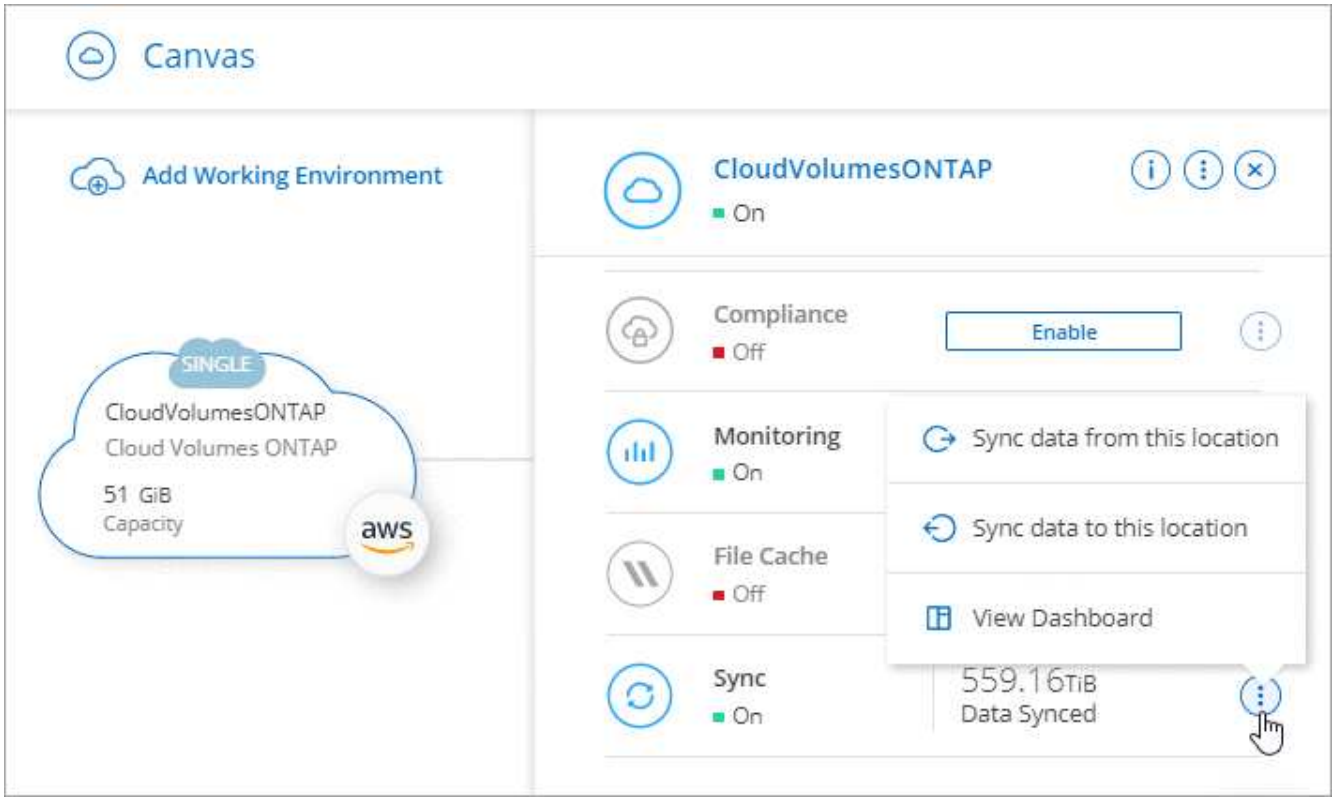
特定の種類のシステムの同期関係を作成する

次のいずれかの同期関係を作成する場合は、まずシステムを作成または検出する必要があります。

- Amazon FSx for ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- オンプレミスのONTAPクラスター

手順

1. "コピーと同期にログイン" 。
2. システムを作成または検出します。
   - "Amazon FSx for ONTAPシステムを作成する"
   - "Azure NetApp Files の設定と検出"
   - "AWS でCloud Volumes ONTAP を起動"
   - "Azure でCloud Volumes ONTAP を起動する"
   - "Google Cloud でCloud Volumes ONTAP を起動"
   - "既存のCloud Volumes ONTAPシステムの追加"
   - "ONTAPクラスターの検出"
3. *システムページ*を選択します。
4. 上記のいずれかのタイプに一致するシステムを選択してください。
5. [同期]の横にあるアクション メニューを選択します。



6. *この場所からデータを同期*または*この場所にデータを同期*を選択し、プロンプトに従って同期関係を設定します。

他の種類の同期関係を作成する

Amazon FSx for ONTAP、 Azure NetApp Files、 Cloud Volumes ONTAP、またはオンプレミスのONTAPクラスター以外のサポートされているストレージタイプとの間でデータを同期するには、次の手順に従います。以下の手順は、NFS サーバーから S3 バケットへの同期関係を設定する方法を示した例です。

1. NetApp Consoleで、[同期] を選択します。
2. *同期関係の定義*ページで、ソースとターゲットを選択します。

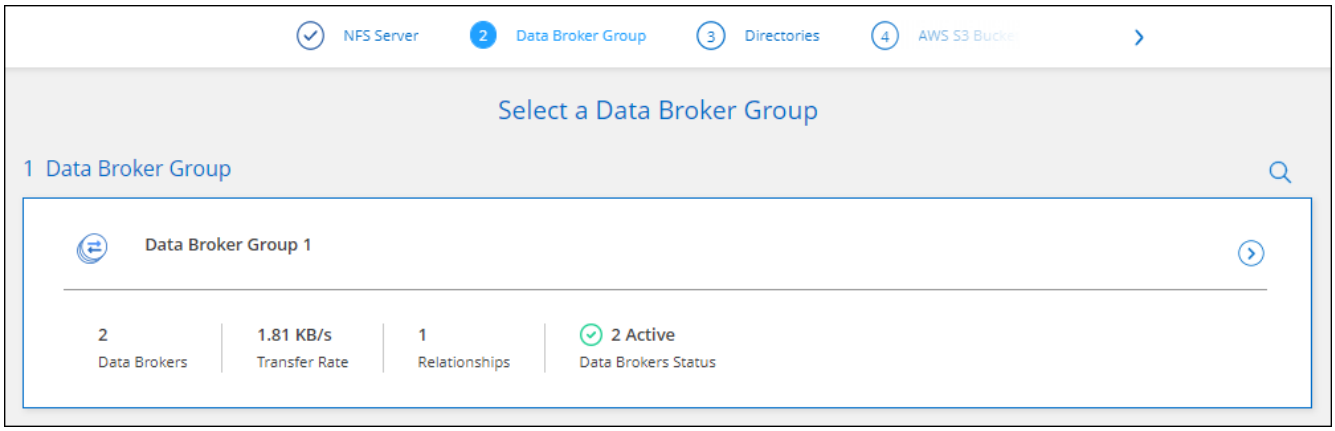
   次の手順は、NFS サーバーから S3 バケットへの同期関係を作成する方法の例を示しています。

3. **NFS** サーバー ページで、AWS に同期する NFS サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。
4. データ ブローカー グループ ページで、プロンプトに従って、AWS、Azure、または Google Cloud Platform にデータ ブローカー仮想マシンを作成するか、既存の Linux ホストにデータ ブローカー ソフトウェアをインストールします。

   詳細については、次のページを参照してください。

- "AWSでデータブローカーを作成する"
- "Azureでデータブローカーを作成する"
- "Google Cloud でデータ ブローカーを作成する"
- "Linuxホストへのデータブローカーのインストール"

5. データ ブローカーをインストールしたら、[続行] を選択します。

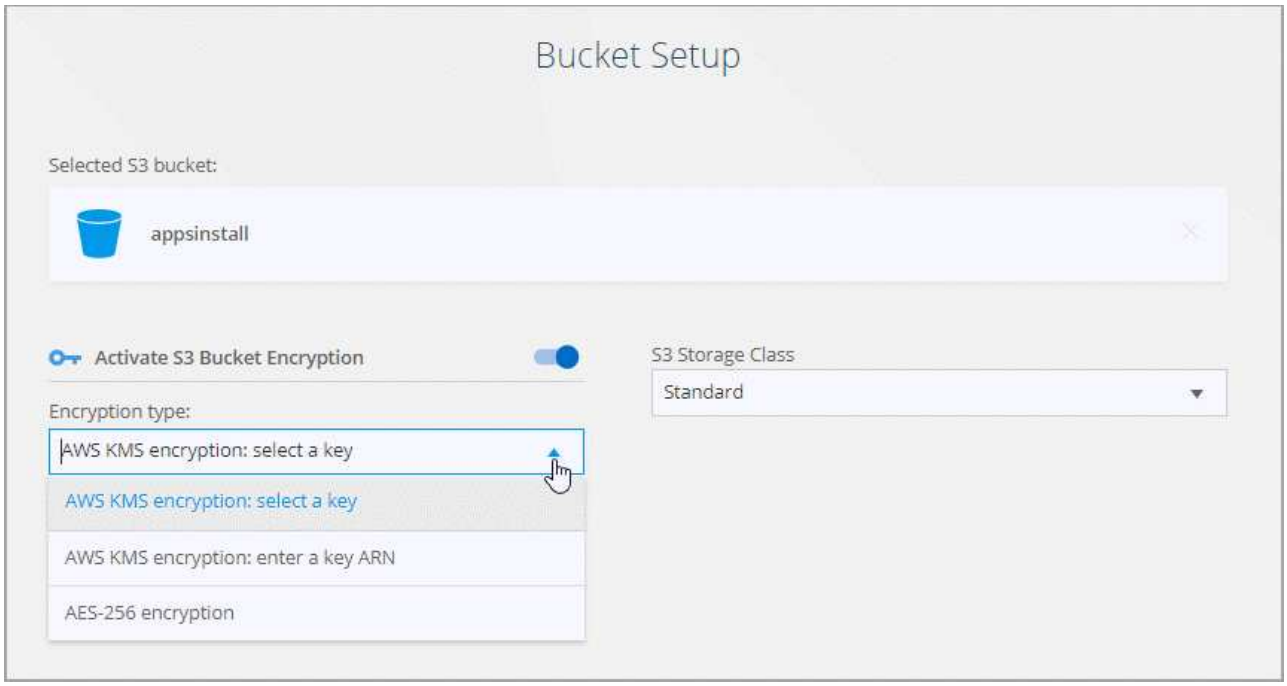


6. *ディレクトリ*ページで、最上位ディレクトリまたはサブディレクトリを選択します。

コピーと同期でエクスポートを取得できない場合は、「エクスポートを手動で追加」を選択し、NFS エクスポートの名前を入力します。

NFS サーバー上の複数のディレクトリを同期する場合は、完了後に追加の同期関係を作成する必要があります。

7. **AWS S3** バケット ページで、バケットを選択します。
   - ドリルダウンしてバケット内の既存のフォルダを選択するか、バケット内に作成した新しいフォルダを選択します。
   - AWS アカウントに関連付けられていない S3 バケットを選択するには、[リストに追加] を選択します。"S3バケットに特定の権限を適用する必要がある" 。
8. *バケット設定*ページでバケットを設定します。
   - S3 バケット暗号化を有効にするかどうかを選択し、AWS KMS キーを選択するか、KMS キーの ARN を入力するか、AES-256 暗号化を選択します。
   - S3 ストレージクラスを選択します。"サポートされているストレージクラスを表示する" 。



9. *設定*ページで、ソースファイルとフォルダをターゲットの場所で同期および維持する方法を定義します。

スケジュール

今後の同期の定期スケジュールを選択するか、同期スケジュールをオフにします。関係を 1 分ごとに同期するようにスケジュールできます。

同期タイムアウト

指定された分数、時間数、または日数内に同期が完了しなかった場合に、コピーと同期でデータ同期をキャンセルするかどうかを定義します。

通知

NetAppコンソールの通知センターでコピーと同期の通知を受信するかどうかを選択できます。成功したデータ同期、失敗したデータ同期、キャンセルされたデータ同期に関する通知を有効にすることができます。

再試行

コピーと同期がファイルをスキップする前に同期を再試行する回数を定義します。

連続同期

最初のデータ同期の後、コピーと同期はソースの S3 バケットまたは Google Cloud Storage バケットの変更をリッスンし、変更が発生するたびにターゲットに継続的に同期します。スケジュールされた間隔でソースを再スキャンする必要はありません。

この設定は、同期関係を作成するとき、および S3 バケットまたは Google Cloud Storage から Azure Blob Storage、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、S3、 StorageGRIDに、または Azure Blob Storage から Azure Blob Storage、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、 StorageGRIDにデータを同期する場合にのみ使用できます。

この設定を有効にすると、他の機能に次の影響があります。

- 同期スケジュールは無効です。
- 次の設定はデフォルト値に戻ります: 同期タイムアウト、最近変更されたファイル、および変更日。
- S3 がソースの場合、サイズによるフィルターはコピー イベントでのみアクティブになります (削除イベントではアクティブになりません)。
- 関係が作成された後は、関係を加速するか削除することしかできません。同期を中止したり、設定を変更したり、レポートを表示したりすることはできません。

  外部バケットとの継続的な同期関係を作成できます。これを行うには、次の手順に従ってください。

  i. 外部バケットのプロジェクトの Google Cloud コンソールに移動します。

  ii. クラウド ストレージ > 設定 > クラウド ストレージ サービス アカウント に移動します。

  iii. local.json ファイルを更新します。

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

  iv. データ ブローカーを再起動します。

    A. sudo pm2 すべて停止

    B. sudo pm2 すべて開始

  v. 関連する外部バケットとの継続的な同期関係を作成します。

> ⓘ 外部バケットとの継続的な同期関係を作成するために使用されるデータ ブローカーは、プロジェクト内のバケットとの別の継続的な同期関係を作成することはできません。

比較する

ファイルまたはディレクトリが変更されたかどうか、再度同期する必要があるかどうかを判断するときに、コピーと同期で特定の属性を比較するかどうかを選択します。

これらの属性のチェックを外しても、コピーと同期はパス、ファイル サイズ、ファイル名をチェックしてソースとターゲットを比較します。変更があった場合は、それらのファイルとディレクトリが同期されます。

次の属性を比較して、コピーと同期を有効にするか無効にするかを選択できます。

- **mtime**: ファイルの最終更新時刻。この属性はディレクトリには無効です。
- **uid**、**gid**、および **mode**: Linux の権限フラグ。

オブジェクトのコピー

オブジェクト ストレージのメタデータとタグをコピーするには、このオプションを有効にします。ユーザーがソースのメタデータを変更した場合、コピーと同期は次の同期でこのオブジェクトをコピーしますが、ユーザーがソースのタグを変更した場合 (データ自体ではなく)、コピーと同期は次の同期でオブジェクトをコピーしません。

関係を作成した後は、このオプションを編集することはできません。

タグのコピーは、Azure Blob または S3 互換エンドポイント (S3、 StorageGRID、または IBM Cloud Object Storage) をターゲットとして含む同期関係でサポートされます。

メタデータのコピーは、次のいずれかのエンドポイント間の「クラウド間」関係でサポートされます。

- AWS S3
- Azure ブロブ
- Google Cloud Storage
- IBM Cloud Object Storage
- StorageGRID

最近変更されたファイル

スケジュールされた同期の前に最近変更されたファイルを除外することを選択します。

ソース上のファイルを削除

コピーと同期によってファイルがターゲットの場所にコピーされた後、ソースの場所からファイルを削除することを選択します。このオプションでは、ソース ファイルがコピー後に削除されるため、データが失われるリスクがあります。

このオプションを有効にする場合は、データ ブローカーの local.json ファイル内のパラメーターも変更する必要があります。ファイルを開き、次のように更新します。

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

local.json ファイルを更新した後、再起動する必要があります。 `pm2 restart all` 。

ターゲット上のファイルを削除する

ソースからファイルが削除された場合は、ターゲットの場所からファイルを削除することを選択します。デフォルトでは、ターゲットの場所からファイルを削除しません。

ファイルの種類

各同期に含めるファイルの種類（ファイル、ディレクトリ、シンボリック リンク、ハード リンク）を

定義します。

> ハード リンクは、セキュリティ保護されていない NFS と NFS の関係でのみ使用できます。ユーザーは 1 つのスキャナー プロセスと 1 つのスキャナー同時実行に制限され、スキャンはルート ディレクトリから実行する必要があります。

ファイル拡張子を除外する

ファイル拡張子を入力して Enter キーを押すことで、同期から除外する正規表現またはファイル拡張子を指定します。たとえば、*.log ファイルを除外するには、「*log*」または「*.log*」と入力します。複数の拡張子の場合、区切り文字は必要ありません。次のビデオでは短いデモを紹介します。

同期関係のファイル拡張子を除外する

> Regex または正規表現は、ワイルドカードや glob 表現とは異なります。この機能は正規表現でのみ動作します。

ディレクトリを除外する

同期から除外する正規表現またはディレクトリを最大 15 個指定するには、名前またはディレクトリのフル パスを入力して Enter キーを押します。デフォルトでは、.copy-offload、.snapshot、~snapshot ディレクトリは除外されます。

> Regex または正規表現は、ワイルドカードや glob 表現とは異なります。この機能は正規表現でのみ動作します。

ファイル サイズ

サイズに関係なくすべてのファイルを同期するか、特定のサイズ範囲内のファイルのみを同期するかを選択します。

更新日

最終更新日に関係なくすべてのファイル、特定の日付以降、特定の日付前、または時間範囲内で更新されたファイルを選択します。

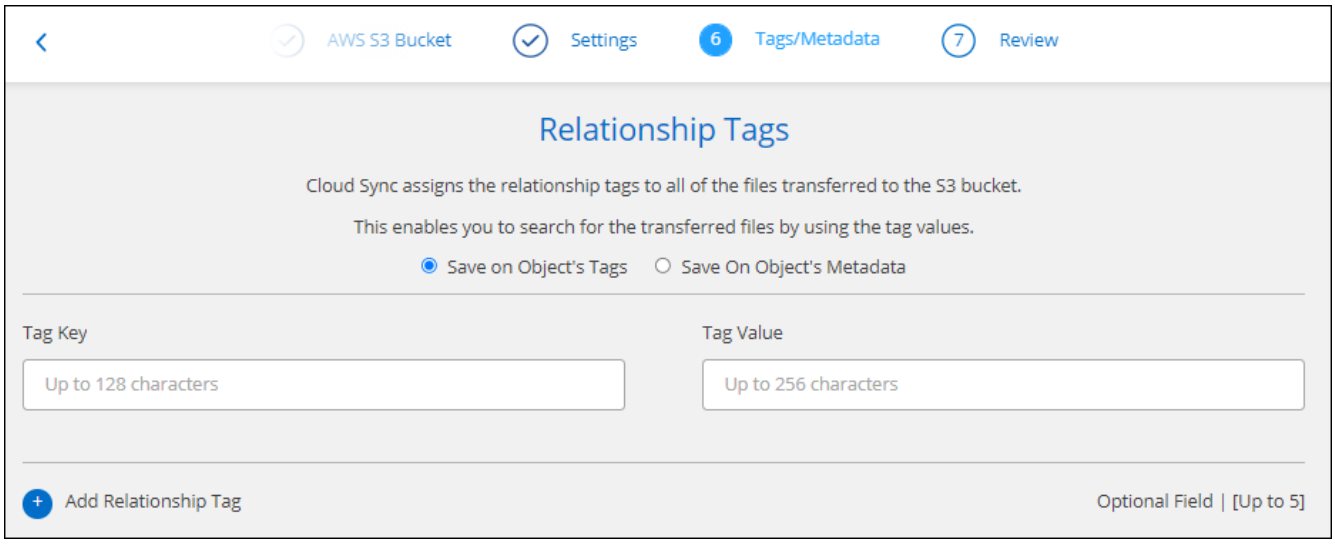
作成日

SMB サーバーがソースの場合、この設定により、特定の日付以降、特定の日付前、または特定の時間範囲内に作成されたファイルを同期できます。

ACL - アクセス制御リスト

関係を作成するとき、または関係を作成した後に設定を有効にして、SMB サーバーから ACL のみ、ファイルのみ、または ACL とファイルをコピーします。

10. *タグ/*メタデータ ページで、S3 バケットに転送されるすべてのファイルにキーと値のペアをタグとして保存するか、すべてのファイルにメタデータのキーと値のペアを割り当てるかを選択します。



同じ機能は、 StorageGRIDおよび IBM Cloud Object Storage にデータを同期するときにも利用できます。 Azure および Google Cloud Storage の場合、メタデータ オプションのみが利用可能です。

11. 同期関係の詳細を確認し、「関係の作成」を選択します。

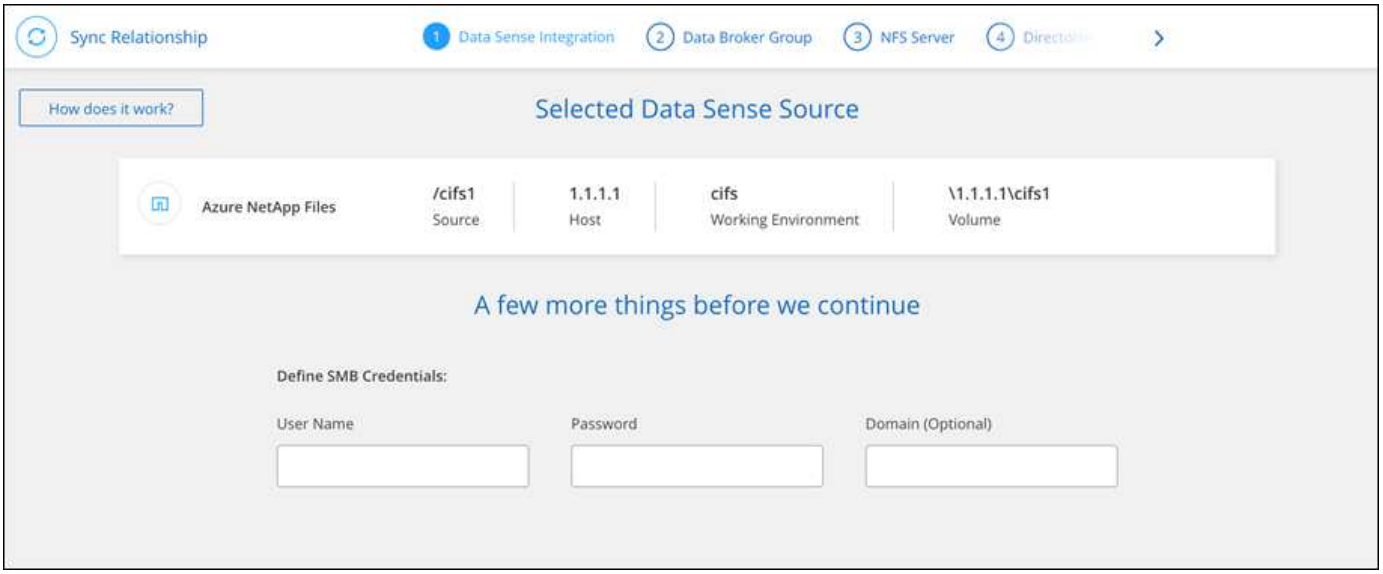
結果

コピーと同期は、ソースとターゲット間のデータの同期を開始します。同期にかかった時間、同期が停止したかどうか、コピー、スキャン、または削除されたファイルの数に関する同期統計が利用できます。その後、 "同期関係" 、 "データブローカーを管理する" 、 または "パフォーマンスと構成を最適化するためのレポートを作成する"。

NetApp Data Classificationから同期関係を作成する

コピーと同期はNetApp Data Classificationと統合されています。 NetApp Data Classification内から、コピーと同期を使用してターゲットの場所に同期するソース ファイルを選択できます。

NetApp Data Classificationからデータ同期を開始すると、すべてのソース情報が 1 つの手順にまとめられ、いくつかの重要な詳細を入力するだけで済みます。次に、新しい同期関係のターゲットの場所を選択します。



"NetApp Data Classificationから同期関係を開始する方法を学びます" 。

NetApp Copy and Syncで SMB 共有から ACL をコピーする

NetApp Copy and Sync は、 SMB 共有間、および SMB 共有とオブジェクト ストレージ (ONTAP S3 を除く) 間でアクセス制御リスト (ACL) をコピーできます。必要に応じて、robocopy を使用して SMB 共有間の ACL を手動で保持することもできます。

オプション

- コピーと同期を設定して ACL を自動的にコピーする
- SMB共有間でACLを手動でコピーする

ACLをコピーするにはコピーと同期を設定する

関係を作成するとき、または関係を作成した後に設定を有効にして、SMB 共有間および SMB 共有とオブジェクト ストレージ間で ACL をコピーします。

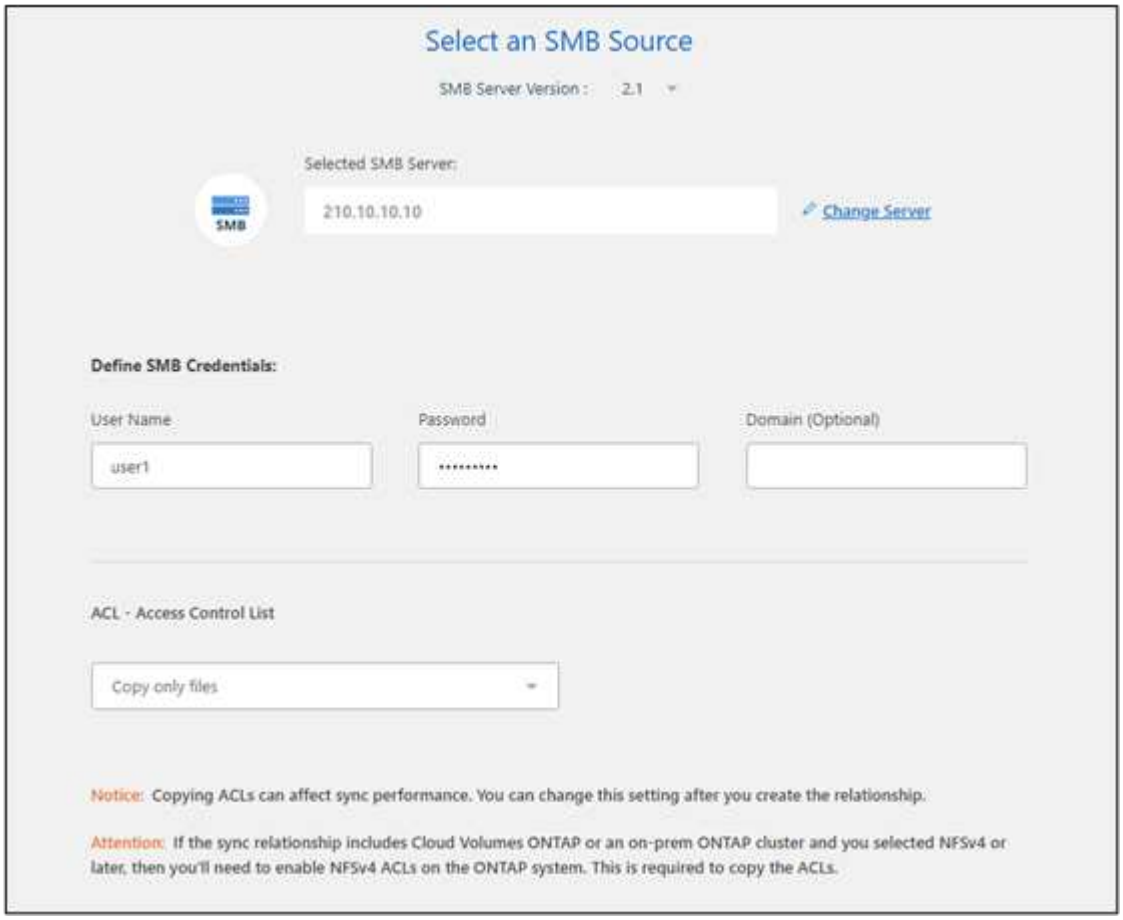
開始する前に

この機能は、AWS、Azure、Google Cloud Platform、オンプレミスのデータブローカーなど、あらゆるタイプのデータブローカーで動作します。オンプレミスのデータブローカーは、"サポートされているオペレーティングシステム" 。

新しい関係を築くためのステップ

1. "コピーと同期にログイン" 。
2. 「コピーと同期」から、「新しい同期の作成」を選択します。
3. SMB サーバーまたはオブジェクト ストレージをソースとして、SMB サーバーまたはオブジェクト ストレージをターゲットとしてドラッグ アンド ドロップし、[続行] を選択します。
4. **SMB** サーバー ページで:
   a. 新しい SMB サーバーを入力するか、既存のサーバーを選択して [続行] を選択します。
   b. SMB サーバーの資格情報を入力します。

c. ファイルのみコピー、**ACL** のみコピー、ファイルと **ACL** をコピー のいずれかを選択し、続行 を選択します。



5. 残りの指示に従って同期関係を作成します。

SMB からオブジェクト ストレージに ACL をコピーする場合、ターゲットに応じて、ACL をオブジェクトのタグにコピーするか、オブジェクトのメタデータにコピーするかを選択できます。 Azure および Google Cloud Storage の場合、メタデータ オプションのみが利用可能です。

次のスクリーンショットは、この選択を行うことができる手順の例を示しています。

既存の関係のための手順

1. 同期関係にマウスを移動し、アクション メニューを選択します。
2. *設定*を選択します。
3. ファイルのみコピー、**ACL** のみコピー、ファイルと **ACL** をコピー のいずれかを選択し、続行 を選択します。
4. *設定を保存*を選択します。

> コピーと同期では SMB ACL (アクセス許可) は保持されますが、ファイルまたはフォルダーの所有権はコピーされません。所有権は SMB ACL 転送操作には含まれません。

結果

データを同期する際、コピーと同期はソースとターゲット間の ACL を保持します。

SMB共有間で**ACL**を手動でコピーする

Windows robocopy コマンドを使用して、SMB 共有間の ACL を手動で保持できます。

> ACLに加えて所有権（所有者とグループ）を保持する必要がある場合は、 `robocopy`指示。使用して `/copyall`フラグは ACL、所有権、監査情報をコピーします。

手順

1. 両方の SMB 共有に完全にアクセスできる Windows ホストを特定します。
2. いずれかのエンドポイントで認証が必要な場合は、**net use** コマンドを使用して Windows ホストからエンドポイントに接続します。

   robocopy を使用する前にこの手順を実行する必要があります。
3. 「コピーと同期」から、ソースとターゲットの SMB 共有間に新しい関係を作成するか、既存の関係を同期します。
4. データ同期が完了したら、Windows ホストから次のコマンドを実行して、ACL と所有権を同期します。

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

   source と *target* は両方とも UNC 形式を使用して指定する必要があります。例: \\<サーバー>\<共有>\<パス>

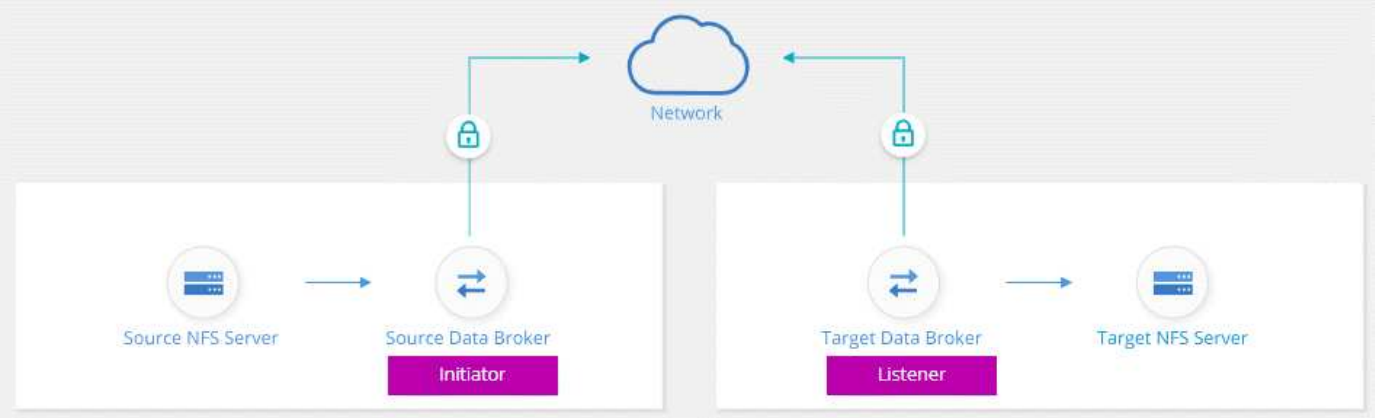
NetApp Copy and Syncの Data In Flight 暗号化を使用して NFS データを同期する

企業に厳格なセキュリティ ポリシーがある場合は、 NetApp Copy and Syncの転送中データ暗号化を使用して NFS データを同期できます。この機能は、NFS サーバーから別の NFS サーバー、およびAzure NetApp FilesからAzure NetApp Files間でサポートされます。

たとえば、異なるネットワークにある 2 つの NFS サーバー間でデータを同期したい場合があります。あるいは、サブネットまたはリージョン間でAzure NetApp Files上のデータを安全に転送する必要がある場合もあります。

転送中のデータ暗号化の仕組み

データインフライト暗号化は、2 つのデータ ブローカー間でネットワーク経由で送信される NFS データを暗号化します。次の図は、2 つの NFS サーバーと 2 つのデータ ブローカーの関係を示しています。



1 つのデータ ブローカーが イニシエーター として機能します。データを同期する時間になると、他のデータ ブローカー (リスナー) に接続要求を送信します。そのデータ ブローカーはポート 443 で要求をリッスンします。必要に応じて別のポートを使用することもできますが、そのポートが別のサービスによって使用されていないことを必ず確認してください。

たとえば、オンプレミスの NFS サーバーからクラウドベースの NFS サーバーにデータを同期する場合、接続要求をリッスンするデータ ブローカーと接続要求を送信するデータ ブローカーを選択できます。

飛行中の暗号化の仕組みは次のとおりです。

1. 同期関係を作成すると、イニシエーターは他のデータ ブローカーとの暗号化された接続を開始します。
2. ソース データ ブローカーは、TLS 1.3 を使用してソースからのデータを暗号化します。
3. 次に、データをネットワーク経由でターゲットのデータ ブローカーに送信します。
4. ターゲット データ ブローカーは、データをターゲットに送信する前に復号化します。
5. 最初のコピーの後、コピーと同期は変更されたデータを 24 時間ごとに同期します。同期するデータがある場合、イニシエーターが他のデータ ブローカーとの暗号化された接続を開くことでプロセスが開始されます。

   より頻繁にデータを同期したい場合は、"関係を作成した後でもスケジュールを変更できます" 。

サポートされる**NFS**バージョン

- NFS サーバーの場合、データインフライト暗号化は NFS バージョン 3、4.0、4.1、および 4.2 でサポートされます。
- Azure NetApp Filesの場合、データインフライト暗号化は NFS バージョン 3 および 4.1 でサポートされます。

プロキシサーバーの制限

暗号化された同期関係を作成すると、暗号化されたデータは HTTPS 経由で送信され、プロキシ サーバー経由でルーティングできなくなります。

始めるために必要なもの

以下のものを必ず用意してください。

- 2つのNFSサーバーが"ソースとターゲットの要件"または、2 つのサブネットまたはリージョンにAzure NetApp Files。
- サーバーの IP アドレスまたは完全修飾ドメイン名。
- 2 つのデータ ブローカーのネットワークの場所。

  既存のデータ ブローカーを選択できますが、イニシエーターとして機能する必要があります。リスナー データ ブローカーは、新しいデータ ブローカーである必要があります。

  既存のデータ ブローカー グループを使用する場合は、グループに含まれるデータ ブローカーが 1 つだけである必要があります。暗号化された同期関係では、グループ内の複数のデータ ブローカーはサポートされません。

  データ ブローカーをまだデプロイしていない場合は、データ ブローカーの要件を確認してください。厳格なセキュリティポリシーがあるため、ポート443からの送信トラフィックと、"インターネットエンドポイント"データブローカーが連絡する。

  - "AWSのインストールを確認する"
  - "Azureのインストールを確認する"
  - "Google Cloud のインストールを確認する"
  - "Linuxホストのインストールを確認する"

データインフライト暗号化を使用して **NFS** データを同期する

2 つの NFS サーバー間またはAzure NetApp Files間で新しい同期関係を作成し、インフライト暗号化オプションを有効にして、プロンプトに従います。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. **NFS** サーバー をソースとターゲットの場所にドラッグ アンド ドロップするか、* Azure NetApp Files* をソースとターゲットの場所にドラッグ アンド ドロップし、はい を選択して、転送中のデータ暗号化を有効にします。
4. 指示に従って関係を作成します。

   a. **NFS** サーバー/* Azure NetApp Files*: NFS バージョンを選択し、新しい NFS ソースを指定するか、既存のサーバーを選択します。

   b. データ ブローカーの機能の定義: ポートで接続要求を リッスン するデータ ブローカーと、接続を 開始 するデータ ブローカーを定義します。ネットワーク要件に基づいて選択してください。

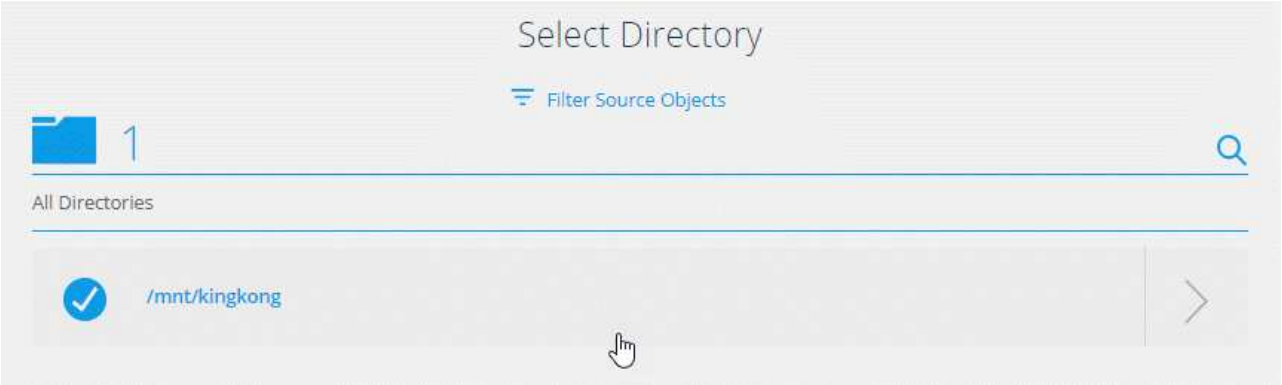
c. データ ブローカー: プロンプトに従って新しいソース データ ブローカーを追加するか、既存のデータ ブローカーを選択します。

   次の点に注意してください。

   - 既存のデータ ブローカー グループを使用する場合は、グループに含まれるデータ ブローカーが 1 つだけである必要があります。暗号化された同期関係では、グループ内の複数のデータ ブローカーはサポートされません。
   - ソース データ ブローカーがリスナーとして機能する場合、それは新しいデータ ブローカーである必要があります。
   - 新しいデータ ブローカーが必要な場合は、Copy and Sync によってインストール手順が表示されます。データ ブローカーをクラウドにデプロイすることも、独自の Linux ホスト用のインストール スクリプトをダウンロードすることもできます。

d. ディレクトリ: すべてのディレクトリを選択するか、ドリルダウンしてサブディレクトリを選択して、同期するディレクトリを選択します。

   ソース ファイルとフォルダーをターゲットの場所で同期および維持する方法を定義する設定を変更するには、[ソース オブジェクトのフィルター] を選択します。

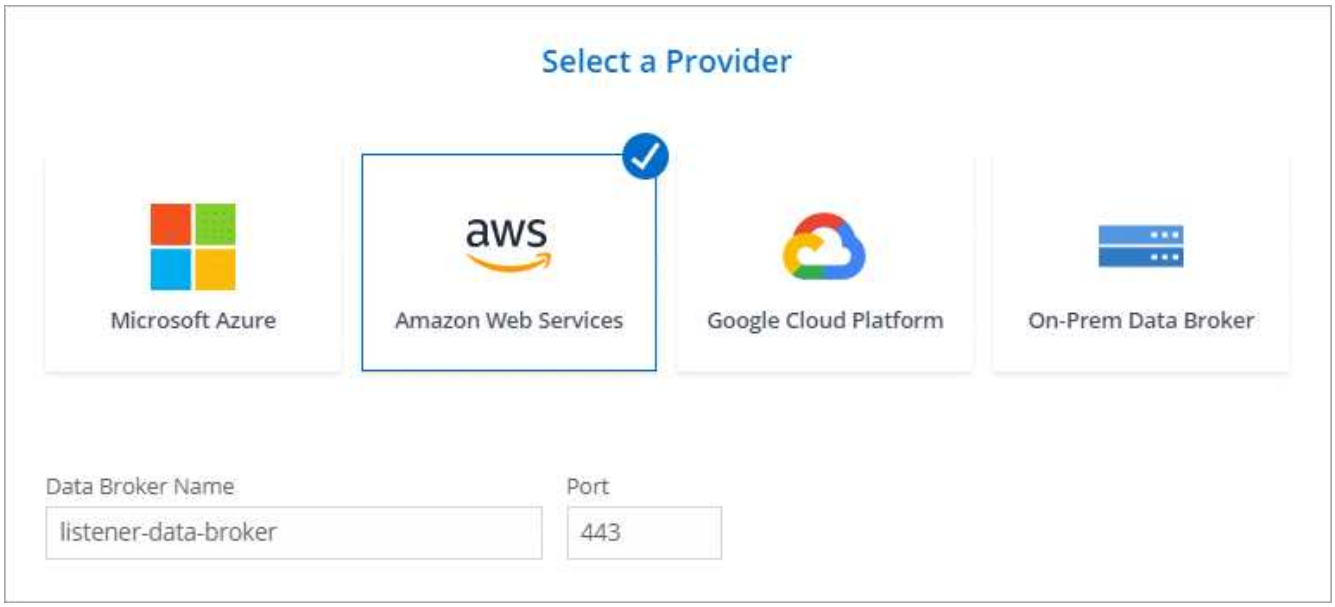


e. ターゲット **NFS** サーバー/ターゲット**Azure NetApp Files**: NFS バージョンを選択し、新しい NFS ターゲットを入力するか、既存のサーバーを選択します。

f. ターゲット データ ブローカー: プロンプトに従って新しいソース データ ブローカーを追加するか、既存のデータ ブローカーを選択します。

   ターゲット データ ブローカーがリスナーとして機能する場合、新しいデータ ブローカーである必要があります。

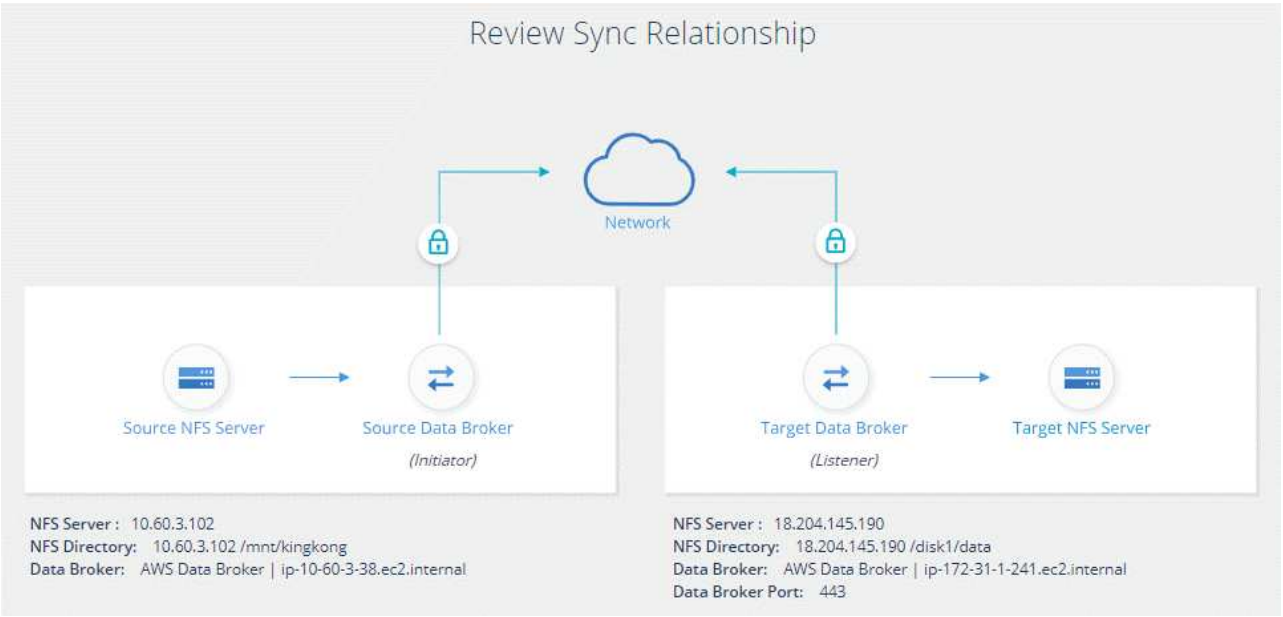
   ターゲット データ ブローカーがリスナーとして機能する場合のプロンプトの例を次に示します。ポートを指定するオプションに注意してください。



a. ターゲット ディレクトリ: 最上位ディレクトリを選択するか、ドリルダウンして既存のサブディレクトリを選択するか、エクスポート内に新しいフォルダーを作成します。

b. 設定: ソース ファイルとフォルダーをターゲットの場所で同期および維持する方法を定義します。

c. 確認: 同期関係の詳細を確認し、[関係の作成] を選択します。



結果

コピーと同期により、新しい同期関係の作成が開始されます。完了したら、[ダッシュボードで表示] を選択して、新しい関係の詳細を表示します。

NetApp Copy and Syncで外部 **HashiCorp Vault** を使用するためのデータ ブローカー グループを設定する

Amazon S3、Azure、または Google Cloud の認証情報を必要とする同期関係を作成する場合は、 NetApp Copy and Syncユーザー インターフェイスまたは API を通じてそれら

の認証情報を指定する必要があります。別の方法としては、データ ブローカー グループを設定して、外部の HashiCorp Vault から資格情報 (または シークレット) に直接アクセスすることもできます。

この機能は、Amazon S3、Azure、または Google Cloud の資格情報を必要とする同期関係を持つコピーおよび同期 API を通じてサポートされます。

1 金庫の準備

URL を設定して、データ ブローカー グループに資格情報を提供するためのボールトを準備します。ボールト内のシークレットの URL は、*Creds* で終わる必要があります。

2 データブローカーグループの準備

グループ内の各データ ブローカーのローカル構成ファイルを変更して、データ ブローカー グループが外部ボールトから資格情報を取得できるように準備します。

3 APIを使用して同期関係を作成する

すべての設定が完了したら、API 呼び出しを送信して、ボールトを使用してシークレットを取得する同期関係を作成できます。

金庫の準備

コピーと同期に、ボールト内のシークレットの URL を提供する必要があります。これらの URL を設定して、Vault を準備します。作成する予定の同期関係の各ソースとターゲットの資格情報への URL を設定する必要があります。

URL は次のように設定する必要があります。

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

パス
: シークレットへのプレフィックス パス。これは、あなたに固有の任意の値にすることができます。

Request ID
: 生成する必要があるリクエスト ID。同期関係を作成するときに、API POST リクエストのヘッダーの 1 つに ID を指定する必要があります。

エンドポイントプロトコル
: 定義される以下のプロトコルのいずれか "ポストリレーションシップv2ドキュメント": S3、AZURE、または GCP (それぞれ大文字にする必要があります)。

資格情報
: URL は *Creds* で終わる必要があります。

例

次の例は、シークレットの URL を示しています。

ソース資格情報の完全な **URL** とパスの例
http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds

例からわかるように、プレフィックス パスは */my-path/all-secrets/*、リクエスト ID は *hb312vdasr2*、ソース エンドポイントは S3 です。

ターゲット資格情報の完全な **URL** とパスの例
http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds

プレフィックス パスは */my-path/all-secrets/*、要求 ID は *n32hcbnejk2*、ターゲット エンドポイントは Azure です。

データブローカーグループの準備

グループ内の各データ ブローカーのローカル構成ファイルを変更して、データ ブローカー グループが外部ボールトから資格情報を取得できるように準備します。

手順

1. グループ内のデータ ブローカーに SSH で接続します。
2. /opt/netapp/databroker/config にある local.json ファイルを編集します。
3. enable を **true** に設定し、*external-integrations.hashicorp* の下の構成パラメータ フィールドを次のように設定します。

   有効
   - 有効な値: true/false
   - タイプ: ブール値
   - デフォルト値: false
   - 真実: データブローカーは独自の外部HashiCorp Vaultから秘密情報を取得します
   - False: データブローカーは資格情報をローカルの保管庫に保存します

   URL
   - タイプ: 文字列
   - 値: 外部の金庫へのURL

   path（パス）
   - タイプ: 文字列
   - 値: シークレットへのパスの先頭に資格情報を入力します

   拒否-不正
   - データブローカーが不正な外部ボールトを拒否するかどうかを決定します
   - タイプ: ブール値
   - デフォルト: false

認証方法
- データブローカーが外部のボールトから資格情報にアクセスするために使用する認証方法
- タイプ: 文字列
- 有効な値: "aws-iam" / "role-app" / "gcp-iam"

ロール名
- タイプ: 文字列
- ロール名（aws-iam または gcp-iam を使用する場合）

シークレットイドとルートイド
- タイプ: 文字列 (app-role を使用する場合)

ネームスペース
- タイプ: 文字列
- 名前空間（必要な場合は X-Vault-Namespace ヘッダー）

4. グループ内の他のデータ ブローカーに対しても、これらの手順を繰り返します。

aws-role認証の例

```
{
        "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 認証の例

```
{
"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 認証を使用する際の権限の設定

gcp-iam 認証方法を使用している場合、データ ブローカーには次の GCP 権限が必要です。

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

"データブローカーの GCP 権限要件の詳細" 。

ボールトからのシークレットを使用して新しい同期関係を作成する

すべての設定が完了したら、API 呼び出しを送信して、ボールトを使用してシークレットを取得する同期関係を作成できます。

コピーおよび同期 REST API を使用して関係を投稿します。

```
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
```

- ユーザートークンとNetApp ConsoleアカウントIDを取得するには、"ドキュメントのこのページを参照してください"。
- 結婚後の体を作るには、 "relationship-v2 API呼び出しを参照してください"。

例

POSTリクエストの例:

```
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の無料トライアル期間終了後は、同期関係の料金が発生します。

NetApp Copy and Syncの 14 日間の無料トライアルが終了した後、同期関係の支払い方法は 2 つあります。最初のオプションは、AWS または Azure から従量課金制または年間払いでサブスクライブすることです。 2 番目のオプションは、 NetAppから直接ライセンスを購入することです。

AWS Marketplace または Azure Marketplace からサブスクライブできます。両方から購読することはできません。

マーケットプレイス サブスクリプションでNetAppのライセンスを使用するオプションがあります。たとえば、同期関係が 25 個ある場合、ライセンスを使用して最初の 20 個の同期関係に対して料金を支払い、残りの 5 個の同期関係については AWS または Azure から従量課金制で支払うことができます。

"ライセンスの仕組みについて詳しくはこちら" 。

無料トライアル終了後すぐにお支払いいただけない場合、追加の関係を作成することはできません。既存の関係は削除されませんが、サブスクライブするかライセンスを入力するまで、変更することはできません。

ライセンスは、 NetApp Consoleサブスクリプションではなく、 NetApp Copy and Syncまたは該当する Web サイトを通じて管理する必要があります。

AWSからサブスクライブ

AWS では従量課金制または年間払いを選択できます。

従量課金制への手順

1. NetApp Consoleのナビゲーション メニューから、**Mobility > Copy and Sync** を選択します。
2. *ライセンス*を選択します。
3. 「AWS」を選択します。
4. *サブスクライブ*を選択し、*続行*を選択します。
5. AWS Marketplace からサブスクライブし、Copy and Sync に再度ログインして登録を完了します。

   次のビデオでそのプロセスが示されています。

   AWS Marketplaceからコピーと同期をサブスクライブする

年間支払いの手順

1. "AWSマーケットプレイスのページへ" 。
2. *購読を続ける*を選択します。
3. 契約オプションを選択し、「契約の作成」を選択します。

Azureからサブスクライブ

Azure では、従量課金制または年間支払いを選択できます。

要件

関連するサブスクリプションで共同作成者または所有者のアクセス許可を持つ Azure ユーザー アカウント。

手順

1. NetApp Consoleのナビゲーション メニューから、**Mobility > Copy and Sync** を選択します。
2. *ライセンス*を選択します。
3. **Azure** を選択します。
4. *サブスクライブ*を選択し、*続行*を選択します。
5. Azure ポータルで、[作成] を選択し、オプションを選択して、[サブスクライブ] を選択します。

   時間ごとに支払う場合は「月払い」、1 年分を前払いする場合は「年払い」を選択します。

6. デプロイが完了したら、通知ポップアップで SaaS リソースの名前を選択します。
7. *アカウントの設定*を選択して、コピーと同期に戻ります。

   次のビデオでそのプロセスが示されています。

   Azure Marketplace からコピーと同期をサブスクライブする

NetAppからライセンスを購入し、コピーと同期に追加します

同期関係の料金を前払いするには、1 つ以上のライセンスを購入し、それをコピーと同期に追加する必要があります。

要件

ライセンスのシリアル番号と、ライセンスが関連付けられているNetAppサポート サイト アカウントのユーザー名とパスワードが必要になります。

手順

1. ライセンスを購入するには、 NetAppへのお問い合わせ にメールを送信してください。
2. "コピーと同期にログイン" 。
3. *ライセンス*を選択します。
4. *ライセンスの追加*を選択し、必要な情報を追加します。
   a. シリアル番号を入力してください。
   b. 追加するライセンスに関連付けられているNetAppサポート サイト アカウントを選択します。
      - アカウントがすでにNetApp Consoleに追加されている場合は、ドロップダウン リストから選択します。
      - アカウントがまだ追加されていない場合は、[**NSS** 資格情報の追加] を選択し、ユーザー名とパスワードを入力して、[登録] を選択し、ドロップダウン リストから選択します。
   c. *追加*を選択します。

ライセンスを更新する

NetAppから購入したコピーおよび同期ライセンスを延長した場合、コピーおよび同期で新しい有効期限は自動的に更新されません。有効期限を更新するには、ライセンスを再度追加する必要があります。ライセンスは、 NetApp Consoleサブスクリプションではなく、Copy and Sync または該当する Web サイトを通じて管理する必要があります。

手順

1. NetApp Consoleのナビゲーション メニューから、**Mobility > Copy and Sync** を選択します。
2. *ライセンス*を選択します。
3. *ライセンスの追加*を選択し、必要な情報を追加します。
   a. シリアル番号を入力してください。
   b. 追加するライセンスに関連付けられているNetAppサポート サイト アカウントを選択します。
   c. *追加*を選択します。

結果

コピーと同期により、既存のライセンスが新しい有効期限で更新されます。

NetApp Copy and Syncでの同期関係の管理

NetApp Copy and Syncでは、データの即時同期、スケジュールの変更などにより、いつでも同期関係を管理できます。

即時データ同期を実行する

次のスケジュールされた同期を待つのではなく、ソースとターゲットの間でデータをすぐに同期できます。

手順

1. "コピーと同期にログイン" 。
2. *ダッシュボード*から同期関係に移動し、 
3. *今すぐ同期*を選択し、*同期*を選択して確認します。

結果

コピーと同期は、関係のデータ同期プロセスを開始します。

同期パフォーマンスを高速化

関係を管理するグループに追加のデータ ブローカーを追加することで、同期関係のパフォーマンスを高速化します。追加のデータ ブローカーは、新しいデータ ブローカーである必要があります。

仕組み

データ ブローカー グループが他の同期関係を管理している場合、グループに追加する新しいデータ ブローカーによって、それらの同期関係のパフォーマンスも向上します。

たとえば、次の 3 つの関係があるとします。

- 関係1はデータブローカーグループAによって管理されます
- 関係2はデータブローカーグループBによって管理されます
- 関係3はデータブローカーグループAによって管理されます

リレーションシップ 1 のパフォーマンスを高速化したいので、新しいデータ ブローカーをデータ ブローカー グループ A に追加します。グループ A は同期リレーションシップ 3 も管理しているため、リレーションシップの同期パフォーマンスも自動的に高速化されます。

手順

1. 関係にある既存のデータ ブローカーの少なくとも 1 つがオンラインであることを確認します。
2. *ダッシュボード*から同期関係に移動し、 
3. *加速*を選択します。
4. 指示に従って新しいデータ ブローカーを作成します。

結果

コピーと同期により、新しいデータ ブローカーがグループに追加されます。次のデータ同期のパフォーマンスが高速化されるはずです。

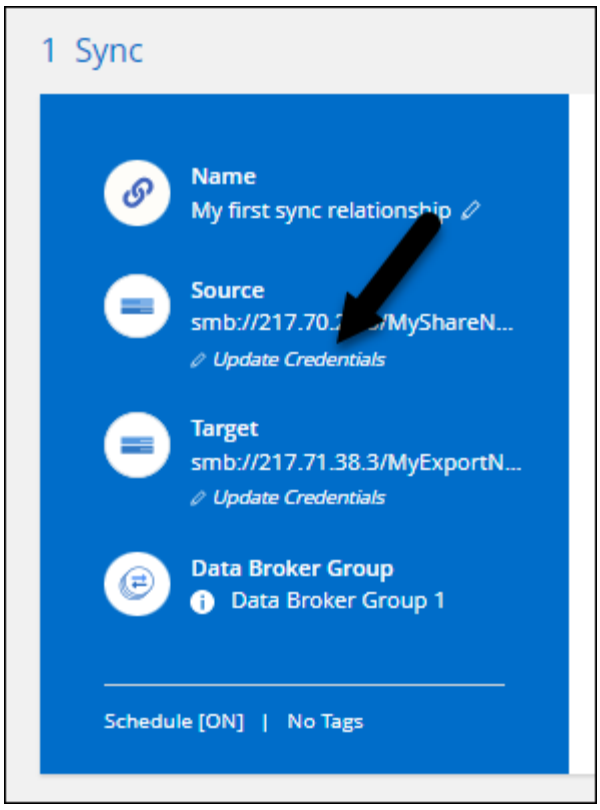
資格情報を更新する

既存の同期関係のソースまたはターゲットの最新の資格情報を使用してデータ ブローカーを更新できます。セキュリティ ポリシーにより定期的に資格情報を更新する必要がある場合は、資格情報を更新すると役立ちます。

資格情報の更新は、コピーと同期で資格情報が必要となるソースまたはターゲット (Azure Blob、Box、IBM Cloud Object Storage、 StorageGRID、 ONTAP S3 ストレージ、SFTP、SMB サーバー) でサポートされています。

手順

1. *同期ダッシュボード*から、資格情報を必要とする同期関係に移動し、*資格情報の更新*を選択します。



2. 資格情報を入力し、「更新」を選択します。

   SMB サーバーに関する注意: ドメインが新しい場合は、資格情報を更新するときにそれを指定する必要があります。ドメインが変更されていない場合は、再度入力する必要はありません。

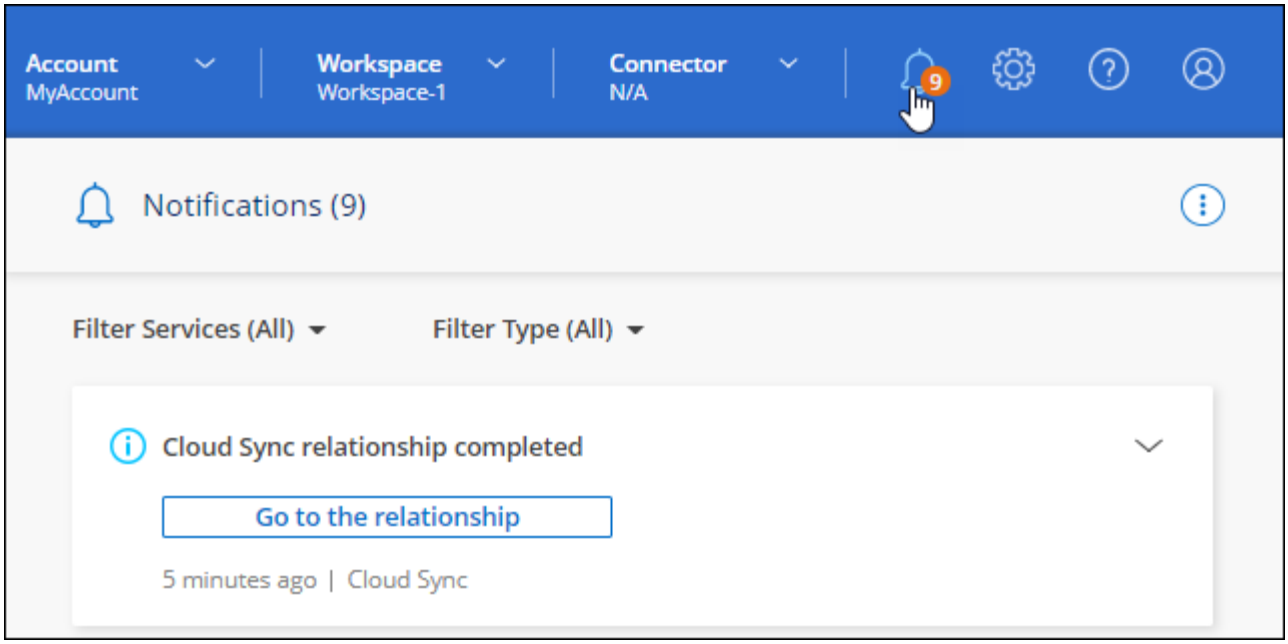
   同期関係を作成するときにドメインを入力したが、資格情報を更新するときに新しいドメインを入力しなかった場合、コピーと同期では、指定した元のドメインが引き続き使用されます。

結果

コピーと同期により、データ ブローカーの資格情報が更新されます。データ ブローカーがデータ同期のために更新された資格情報を使用し始めるまで、最大 10 分かかる場合があります。

通知を設定する

各同期関係の 通知 設定により、 NetAppコンソールの通知センターでコピーと同期の通知を受信するかどうかを選択できます。成功したデータ同期、失敗したデータ同期、キャンセルされたデータ同期に関する通知を有効にすることができます。



また、メールで通知を受け取ることもできます。

手順

1. 同期関係の設定を変更します。
   a. *ダッシュボード*から同期関係に移動し、
   b. *設定*を選択します。
   c. *通知*を有効にします。
   d. *設定を保存*を選択します。
2. 電子メールで通知を受信する場合は、アラートと通知の設定を構成します。
   a. *設定 > アラートと通知の設定*を選択します。
   b. ユーザーまたは複数のユーザーを選択し、「情報」通知タイプを選択します。
   c. *適用*を選択します。

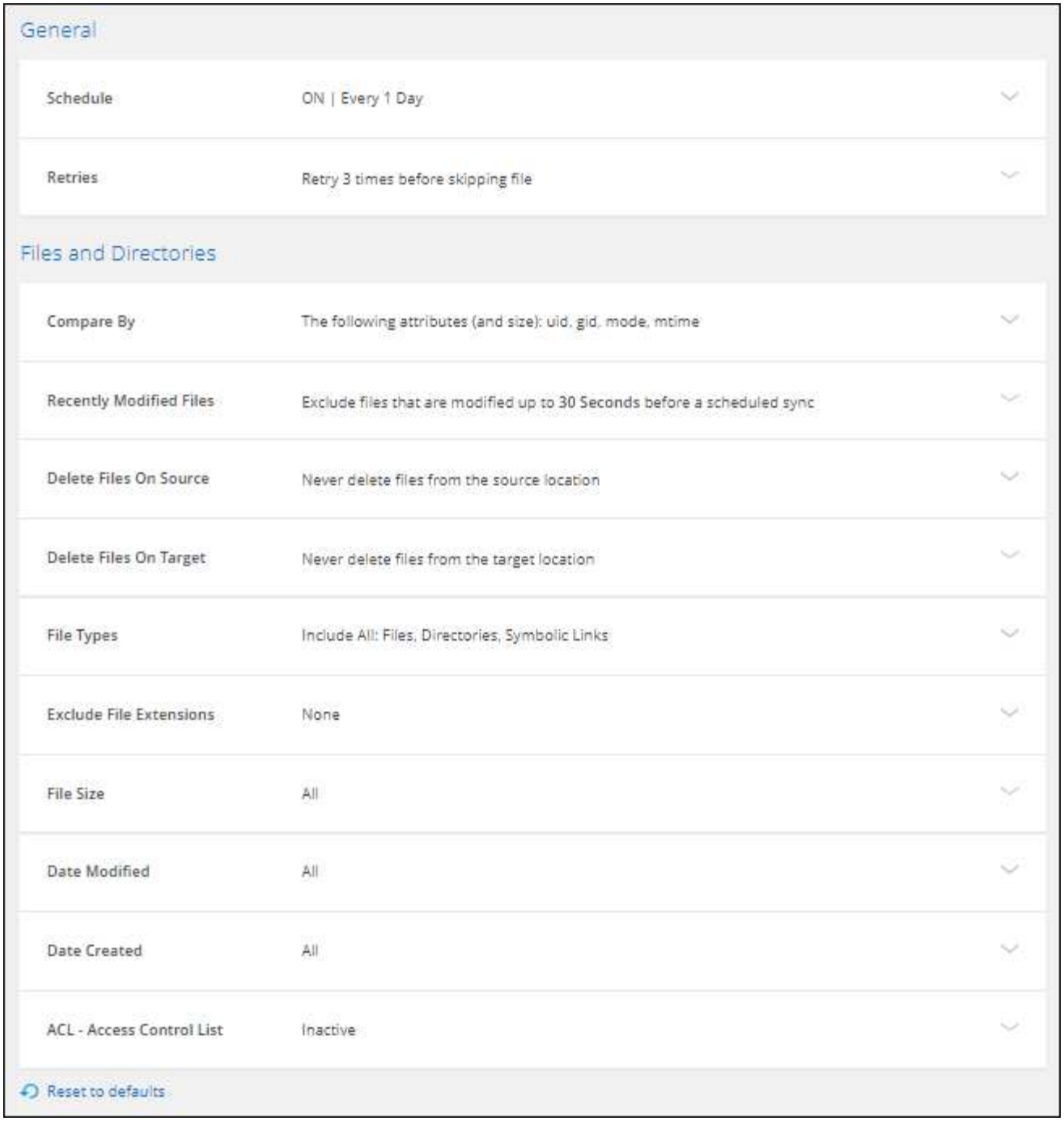
結果

NetAppコンソールの通知センターでコピーと同期の通知が受信されるようになり、オプションを設定している場合は電子メールで通知がいくつか届きます。

同期関係の設定を変更する

ソース ファイルとフォルダーをターゲットの場所で同期および維持する方法を定義する設定を変更します。

1. *ダッシュボード*から同期関係に移動し、
2. *設定*を選択します。
3. いずれかの設定を変更します。



各設定の簡単な説明は次のとおりです。

スケジュール

今後の同期の定期スケジュールを選択するか、同期スケジュールをオフにします。関係を 1 分ごとに同期するようにスケジュールできます。

同期タイムアウト

指定された分数、時間数、または日数内に同期が完了しなかった場合に、コピーと同期でデータ同期をキャンセルするかどうかを定義します。

通知

NetAppコンソールの通知センターでコピーと同期の通知を受信するかどうかを選択できます。成功し

たデータ同期、失敗したデータ同期、キャンセルされたデータ同期に関する通知を有効にすることができます。

通知を受け取りたい場合は

再試行
: コピーと同期がファイルをスキップする前に同期を再試行する回数を定義します。

比較する
: ファイルまたはディレクトリが変更されたかどうか、再度同期する必要があるかどうかを判断するときに、コピーと同期で特定の属性を比較するかどうかを選択します。

これらの属性のチェックを外しても、コピーと同期はパス、ファイル サイズ、ファイル名をチェックしてソースとターゲットを比較します。変更があった場合は、それらのファイルとディレクトリが同期されます。

次の属性を比較して、コピーと同期を有効にするか無効にするかを選択できます。

- **mtime**: ファイルの最終更新時刻。この属性はディレクトリには無効です。
- **uid**、**gid**、および **mode**: Linux の権限フラグ。

オブジェクトのコピー
: 関係を作成した後は、このオプションを編集することはできません。

最近変更されたファイル
: スケジュールされた同期の前に最近変更されたファイルを除外することを選択します。

ソース上のファイルを削除
: コピーと同期によってファイルがターゲットの場所にコピーされた後、ソースの場所からファイルを削除することを選択します。このオプションでは、ソース ファイルがコピー後に削除されるため、データが失われるリスクがあります。

このオプションを有効にする場合は、データ ブローカーの local.json ファイル内のパラメーターも変更する必要があります。ファイルを開き、次のように更新します。

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

local.json ファイルを更新した後、再起動する必要があります。 `pm2 restart all` 。

ターゲット上のファイルを削除する
: ソースからファイルが削除された場合は、ターゲットの場所からファイルを削除することを選択します。デフォルトでは、ターゲットの場所からファイルは削除されません。

ファイルの種類

各同期に含めるファイルの種類（ファイル、ディレクトリ、シンボリック リンク、ハード リンク）を定義します。

ハード リンクは、セキュリティ保護されていない NFS と NFS の関係でのみ使用できます。ユーザーは 1 つのスキャナー プロセスと 1 つのスキャナー同時実行に制限され、スキャンはルート ディレクトリから実行する必要があります。

ファイル拡張子を除外する

ファイル拡張子を入力して Enter キーを押すことで、同期から除外する正規表現またはファイル拡張子を指定します。たとえば、*.log ファイルを除外するには、「*log*」または「*.log*」と入力します。複数の拡張子の場合、区切り文字は必要ありません。次のビデオでは短いデモを紹介します。

同期関係のファイル拡張子を除外する

Regex または正規表現は、ワイルドカードや glob 表現とは異なります。この機能は正規表現でのみ動作します。

ディレクトリを除外する

同期から除外する正規表現またはディレクトリを最大 15 個指定するには、名前またはディレクトリのフル パスを入力して Enter キーを押します。デフォルトでは、.copy-offload、.snapshot、~snapshot ディレクトリは除外されます。

Regex または正規表現は、ワイルドカードや glob 表現とは異なります。この機能は正規表現でのみ動作します。

ファイル サイズ

サイズに関係なくすべてのファイルを同期するか、特定のサイズ範囲内のファイルのみを同期するかを選択します。

更新日

最終更新日に関係なくすべてのファイル、特定の日付以降、特定の日付前、または時間範囲内で更新されたファイルを選択します。

作成日

SMB サーバーがソースの場合、この設定により、特定の日付以降、特定の日付前、または特定の時間範囲内に作成されたファイルを同期できます。

ACL - アクセス制御リスト

関係を作成するとき、または関係を作成した後に設定を有効にして、SMB サーバーから ACL のみ、ファイルのみ、または ACL とファイルをコピーします。

4. *設定を保存*を選択します。

結果

コピーして同期すると、新しい設定で同期関係が変更されます。

関係を削除する

ソースとターゲットの間でデータを同期する必要がなくなった場合は、同期関係を削除できます。このアクションでは、データ ブローカー グループ (または個々のデータ ブローカー インスタンス) は削除されず、ターゲットからデータも削除されません。

オプション**1:** 単一の同期関係を削除する

手順

1. *ダッシュボード*から同期関係に移動し、 
2. *削除*を選択し、もう一度*削除*を選択して確定します。

結果

コピーして同期すると、同期関係が削除されます。

オプション**2:** 複数の同期関係を削除する

手順

1. *ダッシュボード*から「新しい同期を作成」ボタンに移動し、 
2. 削除する同期関係を選択し、「削除」を選択してから、もう一度「削除」を選択して確認します。

結果

コピーして同期すると、同期関係が削除されます。

NetApp Copy and Syncでデータブローカーグループを管理する

NetApp Copy and Syncのデータ ブローカー グループは、ソースの場所からターゲットの場所にデータを同期します。作成する同期関係ごとに、グループ内に少なくとも 1 つのデータ ブローカーが必要です。新しいデータ ブローカーをグループに追加したり、グループに関する情報を表示したりして、データ ブローカー グループを管理します。

データブローカーグループの仕組み

データ ブローカー グループには、1 つ以上のデータ ブローカーを含めることができます。データ ブローカーをグループ化すると、同期関係のパフォーマンスが向上します。

グループは複数の関係を管理できる

データ ブローカー グループは、一度に 1 つ以上の同期関係を管理できます。

たとえば、次の 3 つの関係があるとします。

- 関係1はデータブローカーグループAによって管理されます
- 関係2はデータブローカーグループBによって管理されます

- 関係3はデータブローカーグループAによって管理されます

リレーションシップ 1 のパフォーマンスを高速化したいので、新しいデータ ブローカーをデータ ブローカー グループ A に追加します。グループ A は同期リレーションシップ 3 も管理しているため、リレーションシップの同期パフォーマンスも自動的に高速化されます。

グループ内のデータブローカーの数

多くの場合、単一のデータ ブローカーで同期関係のパフォーマンス要件を満たすことができます。そうでない場合は、グループにデータ ブローカーを追加することで同期のパフォーマンスを向上できます。ただし、まず同期パフォーマンスに影響を与える可能性のある他の要因を確認する必要があります。"複数のデータブローカーが必要な場合の判断方法について詳しくは、こちらをご覧ください。" 。

セキュリティに関する推奨事項

データ ブローカー マシンのセキュリティを確保するために、 NetApp次のことを推奨しています。

- SSHはX11転送を許可しない
- SSHはTCP接続転送を許可しない
- SSHはトンネルを許可しない
- SSHはクライアント環境変数を受け入れてはならない

これらのセキュリティ推奨事項は、データ ブローカー マシンへの不正な接続を防ぐのに役立ちます。

グループに新しいデータブローカーを追加する

新しいデータ ブローカーを作成するには、いくつかの方法があります。

- 新しい同期関係を作成するとき

  "同期関係を作成するときに新しいデータブローカーを作成する方法を学びます" 。

- *データブローカーの管理*ページから*新しいデータブローカーの追加*を選択して、新しいグループにデータブローカーを作成します。
- *データブローカーの管理*ページから、既存のグループに新しいデータブローカーを作成します。

始める前に

- 暗号化された同期関係を管理するグループにデータ ブローカーを追加することはできません。
- 既存のグループにデータ ブローカーを作成する場合、データ ブローカーはオンプレミスのデータ ブローカーまたは同じタイプのデータ ブローカーである必要があります。

  たとえば、グループに AWS データブローカーが含まれている場合は、そのグループ内に AWS データブローカーまたはオンプレミスデータブローカーを作成できます。 Azure データ ブローカーと Google Cloud データ ブローカーは同じデータ ブローカー タイプではないため、作成できません。

新しいグループにデータブローカーを作成する手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。

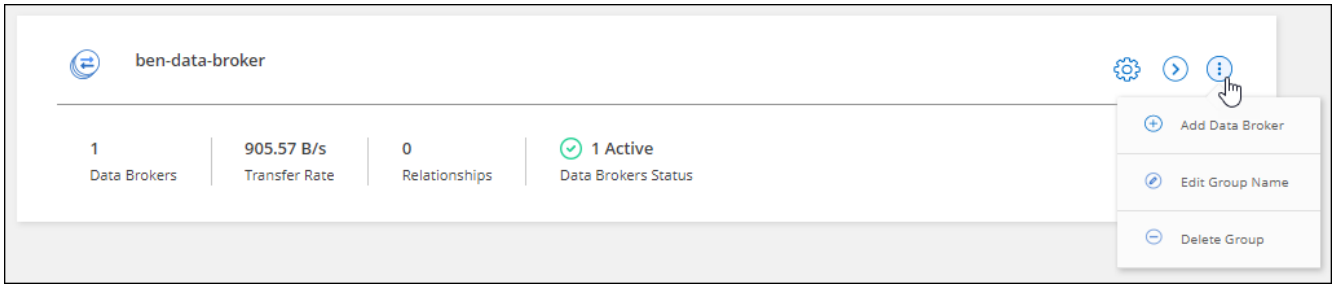
3. *新しいデータブローカーの追加*を選択します。
4. 指示に従ってデータ ブローカーを作成します。

   ヘルプについては、次のページを参照してください。

   - "AWSでデータブローカーを作成する"
   - "Azureでデータブローカーを作成する"
   - "Google Cloud でデータ ブローカーを作成する"
   - "Linuxホストへのデータブローカーのインストール"

既存のグループにデータブローカーを作成する手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。
3. アクション メニューを選択し、データ ブローカーの追加 を選択します。



4. 指示に従ってグループ内にデータ ブローカーを作成します。

   ヘルプについては、次のページを参照してください。

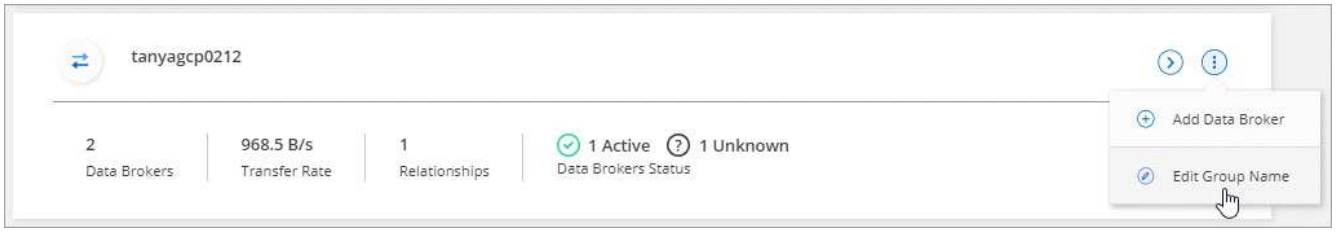
   - "AWSでデータブローカーを作成する"
   - "Azureでデータブローカーを作成する"
   - "Google Cloud でデータ ブローカーを作成する"
   - "Linuxホストへのデータブローカーのインストール"

グループの名前を編集する

データ ブローカー グループの名前はいつでも変更できます。

手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。
3. アクション メニューを選択し、*グループ名の編集*を選択します。



4. 新しい名前を入力し、[保存] を選択します。

結果

コピーと同期により、データ ブローカー グループの名前が更新されます。

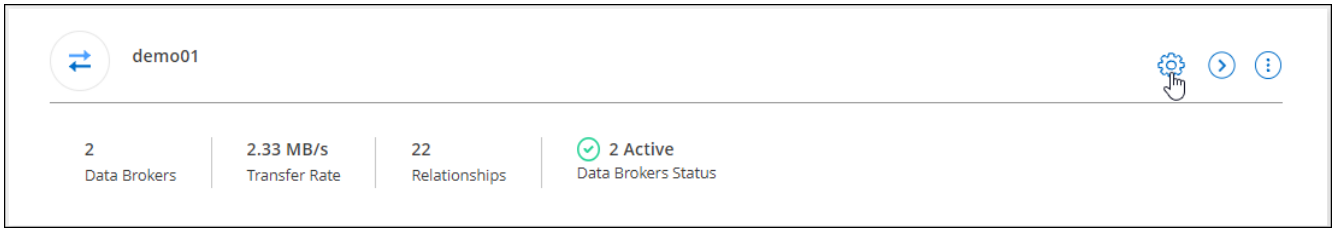
統一された構成を設定する

同期プロセス中に同期関係でエラーが発生した場合、データ ブローカー グループの同時実行性を統合すると、同期エラーの数を減らすことができます。グループの設定を変更すると、転送速度が低下してパフォーマンスに影響する可能性があることに注意してください。

自分で設定を変更することはお勧めしません。構成をいつどのように変更するかについては、 NetAppに相談してください。

手順

1. "コピーと同期にログイン" 。
2. *データブローカーの管理*を選択します。
3. データ ブローカー グループの設定アイコンを選択します。



4. 必要に応じて設定を変更し、「構成の統合」を選択します。

   次の点に注意してください。

   - 変更する設定を選択できます。4 つすべてを一度に変更する必要はありません。
   - 新しい構成がデータ ブローカーに送信されると、データ ブローカーは自動的に再起動し、新しい構成を使用します。
   - この変更が実行され、コピーと同期インターフェースに表示されるまでには、最大 1 分かかる場合があります。
   - データ ブローカーが実行されていない場合、コピーと同期はデータ ブローカーと通信できないため、その構成は変更されません。データ ブローカーを再起動すると、構成が変更されます。
   - 統合構成を設定すると、新しいデータ ブローカーは自動的に新しい構成を使用します。

データブローカーをグループ間で移動する

ターゲット データ ブローカー グループのパフォーマンスを高速化する必要がある場合は、データ ブローカーをあるグループから別のグループに移動します。

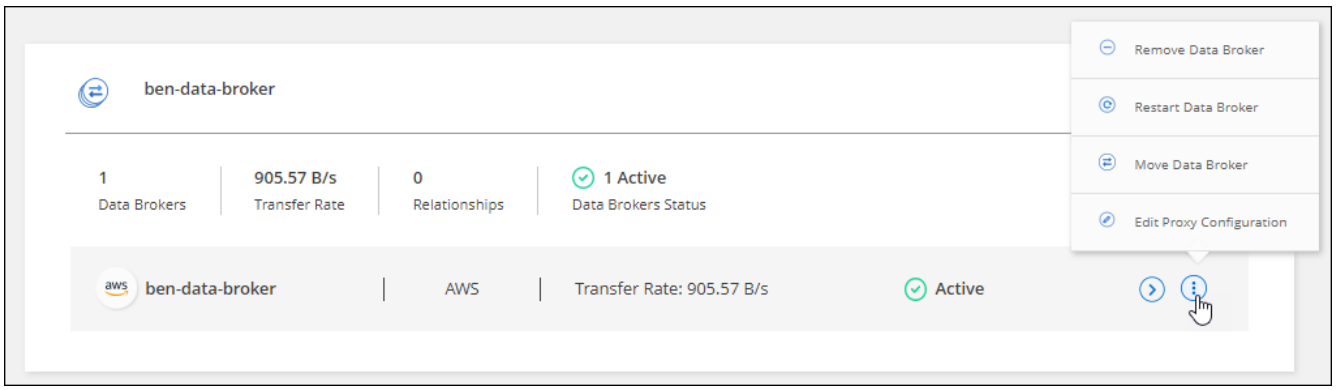
たとえば、データ ブローカーが同期関係を管理しなくなった場合は、同期関係を管理している別のグループに簡単に移動できます。

制限事項

- データ ブローカー グループが同期関係を管理していて、グループ内にデータ ブローカーが 1 つしかない場合は、そのデータ ブローカーを別のグループに移動することはできません。
- 暗号化された同期関係を管理するグループ間でデータ ブローカーを移動することはできません。
- 現在デプロイ中のデータ ブローカーを移動することはできません。

手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。
3. 選択グループ内のデータ ブローカーのリストを展開します。
4. データ ブローカーのアクション メニューを選択し、*データ ブローカーの移動*を選択します。



5. 新しいデータ ブローカー グループを作成するか、既存のデータ ブローカー グループを選択します。
6. *移動*を選択します。

結果

コピーと同期は、データ ブローカーを新規または既存のデータ ブローカー グループに移動します。前のグループに他のデータ ブローカーが存在しない場合は、コピーと同期によってそれが削除されます。

プロキシ設定を更新する

新しいプロキシ構成に関する詳細を追加するか、既存のプロキシ構成を編集して、データ ブローカーのプロキシ構成を更新します。

手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。

3. 選択グループ内のデータ ブローカーのリストを展開します。
4. データ ブローカーのアクション メニューを選択し、*プロキシ構成の編集*を選択します。
5. プロキシの詳細（ホスト名、ポート番号、ユーザー名、パスワード）を指定します。
6. *更新*を選択します。

結果

コピーと同期は、インターネット アクセスにプロキシ構成を使用するようにデータ ブローカーを更新します。

データブローカーの構成を表示する

データ ブローカーの詳細を表示して、ホスト名、IP アドレス、使用可能な CPU や RAM などを確認することができます。

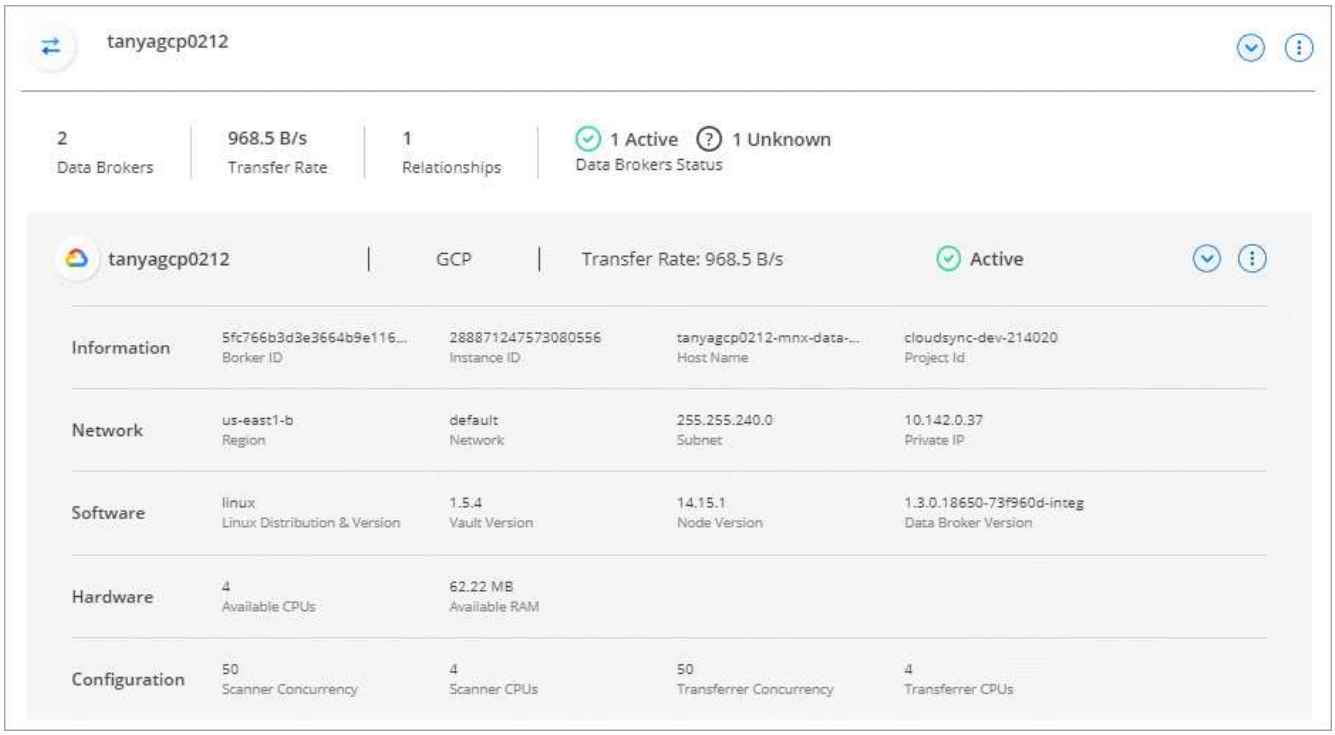
コピーと同期では、データ ブローカーに関する次の詳細が提供されます。

- 基本情報: インスタンス ID、ホスト名など
- ネットワーク: リージョン、ネットワーク、サブネット、プライベート IP など。
- ソフトウェア: Linux ディストリビューション、データ ブローカー バージョンなど。
- ハードウェア: CPUとRAM
- 構成: データブローカーの2種類のメインプロセス（スキャナと転送）の詳細

スキャナーはソースとターゲットをスキャンし、何をコピーするかを決定します。実際のコピーは譲渡者が行います。 NetApp の担当者は、これらの構成の詳細を使用して、パフォーマンスを最適化できるアクションを提案する場合があります。

手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。
3. 選択グループ内のデータ ブローカーのリストを展開します。
4. 選択データ ブローカーの詳細を表示します。

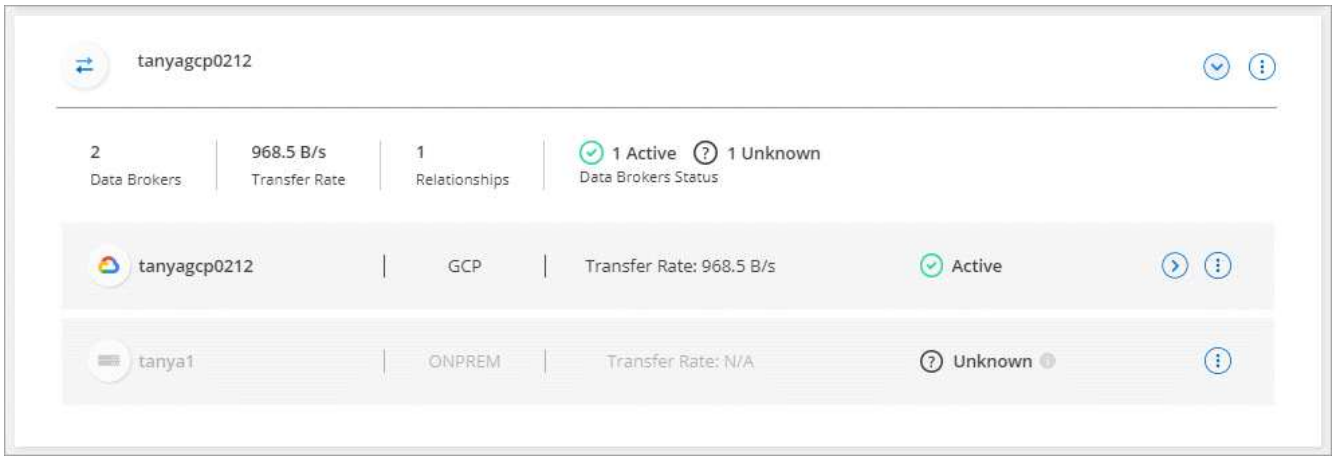


データブローカーの問題に対処する

コピーと同期では、問題のトラブルシューティングに役立つ各データ ブローカーのステータスが表示されます。

手順

1. "コピーと同期にログイン" 。
2. ステータスが「不明」または「失敗」になっているデータ ブローカーを特定します。



3. マウスオーバーしてi失敗の理由を確認するにはアイコンをクリックしてください。
4. 問題を修正してください。

   たとえば、データ ブローカーがオフラインの場合は、データ ブローカーを再起動するだけで済む場合があります。また、最初のデプロイメントが失敗した場合は、データ ブローカーを削除する必要がある場合があります。

グループからデータブローカーを削除する

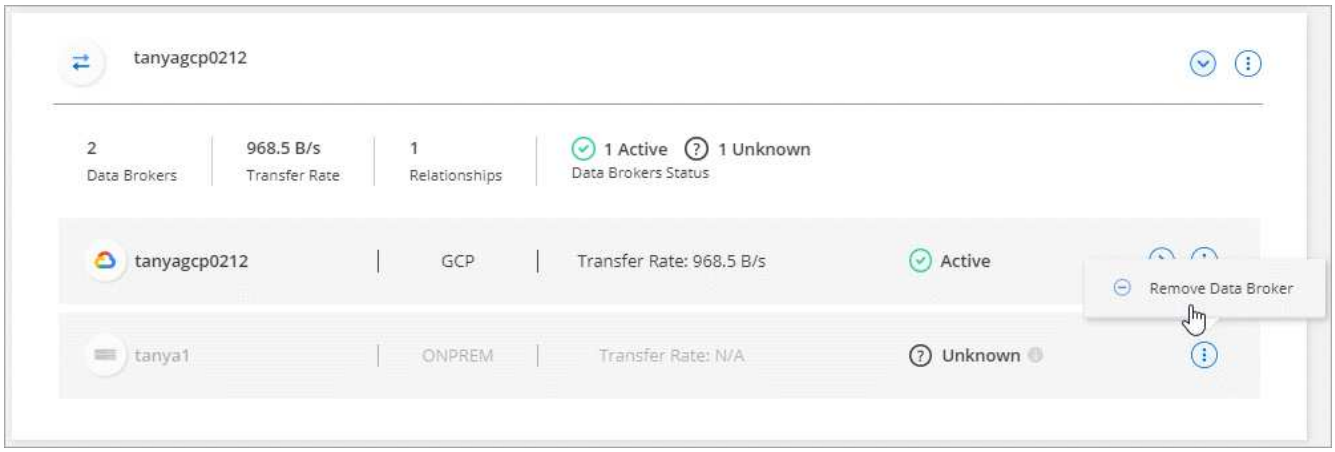
データ ブローカーが不要になった場合、または最初のデプロイメントが失敗した場合は、グループからデータ ブローカーを削除することがあります。このアクションは、コピーと同期のレコードからデータ ブローカーのみを削除します。データ ブローカーと追加のクラウド リソースを手動で削除する必要があります。

知っておくべきこと

- コピーと同期では、グループから最後のデータ ブローカーを削除すると、グループが削除されます。
- そのグループを使用する関係がある場合、グループから最後のデータ ブローカーを削除することはできません。

手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。
3. 選択グループ内のデータ ブローカーのリストを展開します。
4. データ ブローカーのアクション メニューを選択し、*データ ブローカーの削除*を選択します。



5. *データブローカーの削除*を選択します。

結果

コピーと同期により、データ ブローカーがグループから削除されます。

データブローカーグループを削除する

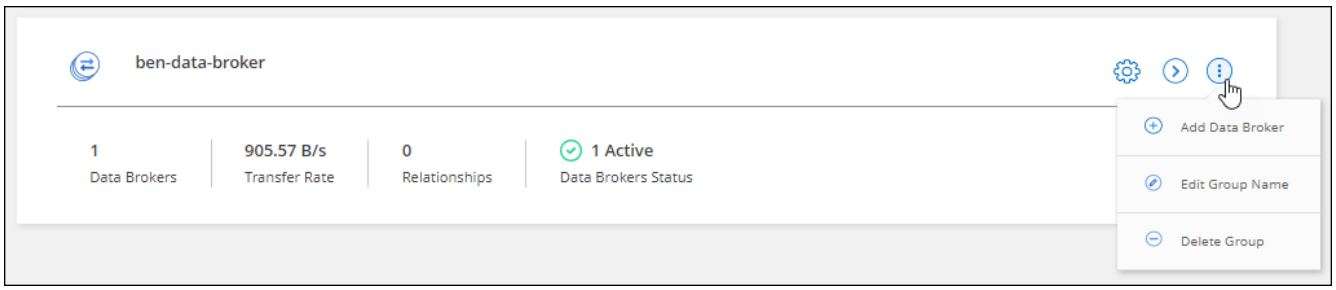
データ ブローカー グループが同期関係を管理しなくなった場合は、グループを削除すると、コピーと同期からすべてのデータ ブローカーが削除されます。

Copy and Sync によって削除されるデータ ブローカーは、Copy and Sync のレコードからのみ削除されます。クラウド プロバイダーと追加のクラウド リソースからデータ ブローカー インスタンスを手動で削除する必要があります。

手順

1. "コピーと同期にログイン" 。
2. *同期 > データブローカーの管理*を選択します。

3. アクション メニューを選択し、*グループの削除*を選択します。



4. 確認するには、グループの名前を入力し、「グループの削除」を選択します。

結果

コピーと同期により、データ ブローカーが削除され、グループが削除されます。

NetApp Copy and Syncで構成を調整するためのレポートを作成して表示します

NetApp Copy and Syncでレポートを作成および表示して、 NetApp担当者の支援を受けてデータ ブローカーの構成を調整し、パフォーマンスを向上させるために使用できる情報を取得します。

各レポートには、同期関係のパスに関する詳細な情報が提供されます。これには、ディレクトリ、ファイル、シンボリック リンクの数、ファイル サイズの分布、ディレクトリの深さと幅、変更時刻、アクセス時刻が含まれます。これは、ダッシュボードから利用できる同期統計とは異なります。 "同期の作成と完了に成功しました" 。

レポートを作成する

レポートを作成するたびに、コピーと同期によってパスがスキャンされ、詳細がレポートにまとめられます。

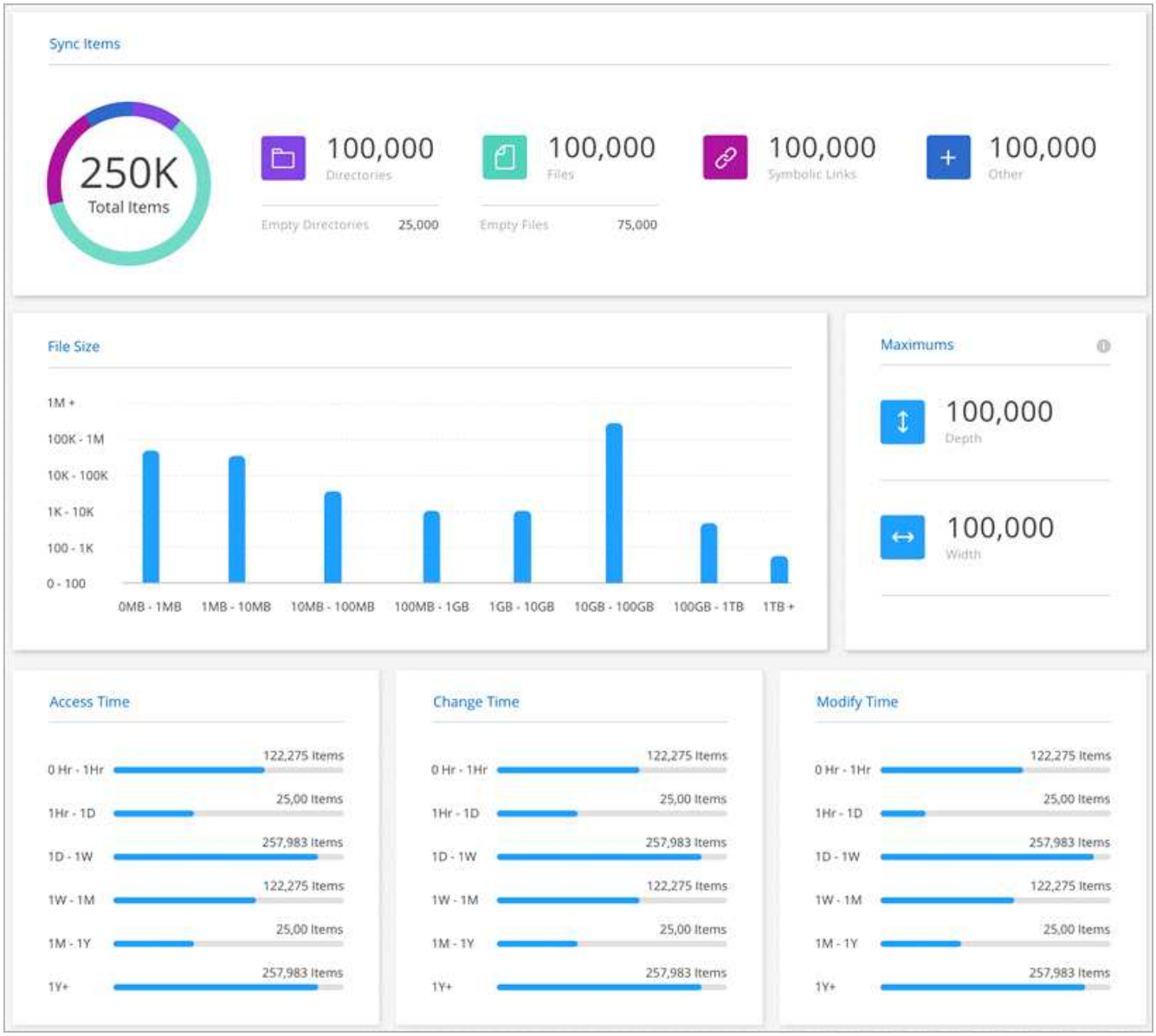
手順

1. "コピーと同期にログイン" 。
2. *同期 > レポート*を選択します。

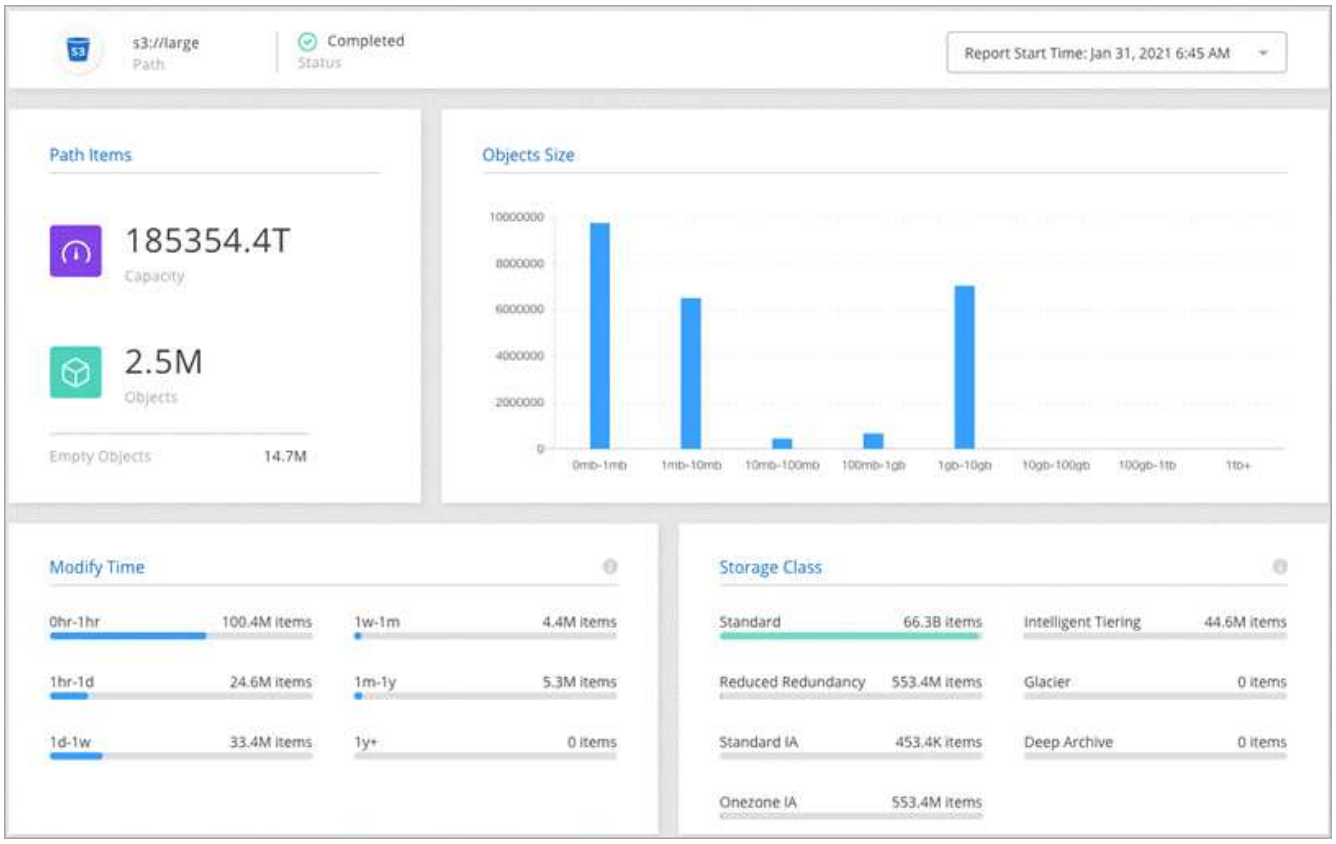
   各同期関係のパス (ソースまたはターゲット) がテーブルに表示されます。

3. レポート アクション 列で、特定のパスに移動して 作成 を選択するか、アクション メニューを選択して 新規作成 を選択します。
4. レポートの準備ができたら、アクション メニューを選択し、[表示] を選択します。

   以下はファイル システム パスのサンプル レポートです。



こちらはオブジェクト ストレージのサンプル レポートです。

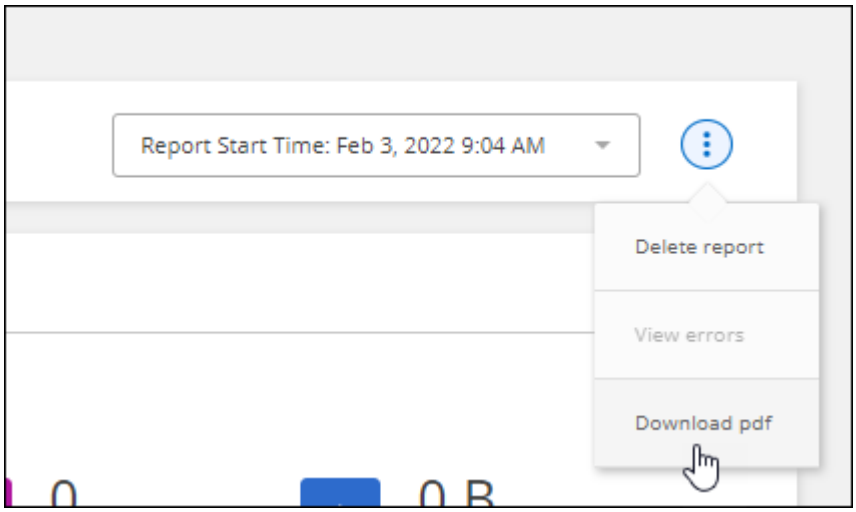


レポートをダウンロード

レポートを PDF 形式でダウンロードして、オフラインで表示したり共有したりすることができます。

手順

1. "コピーと同期にログイン" 。
2. *同期 > レポート*を選択します。
3. レポート アクション 列で、アクション メニューを選択し、表示 を選択します。
4. レポートの右上にあるアクション メニューを選択し、*PDF のダウンロード*を選択します。



レポートエラーを表示

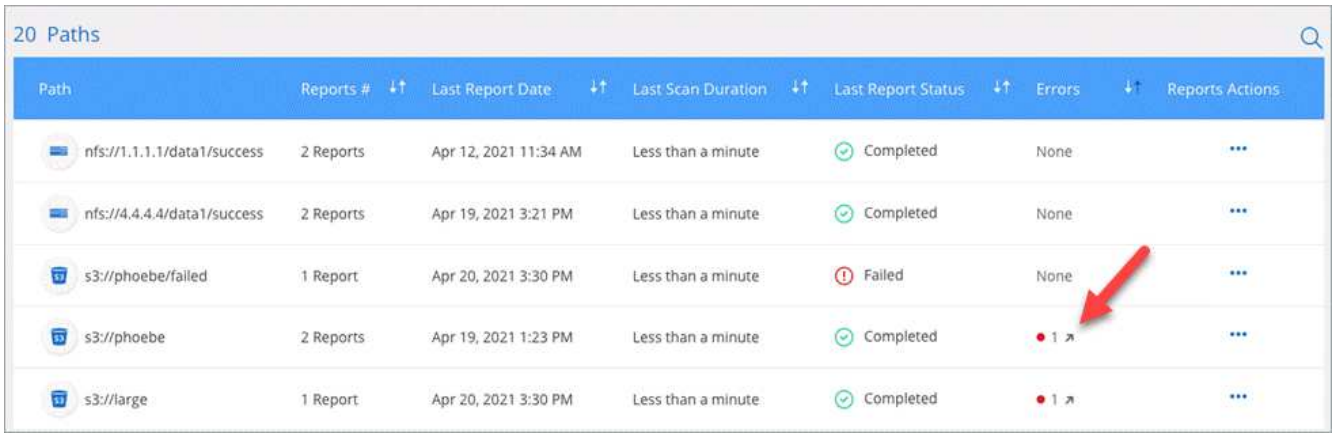
パス テーブルは、最新のレポートにエラーが存在するかどうかを識別します。エラーは、パスをスキャンするときにコピーと同期が直面した問題を識別します。

たとえば、レポートにアクセス権拒否エラーが含まれる場合があります。このタイプのエラーは、コピーと同期がファイルとディレクトリのセット全体をスキャンする機能に影響を与える可能性があります。

エラーのリストを表示した後、問題に対処してレポートを再度実行できます。

手順

1. "コピーと同期にログイン" 。
2. *同期 > レポート*を選択します。
3. *エラー*列で、レポートにエラーが存在するかどうかを確認します。
4. エラーがある場合は、エラー数の横にある矢印を選択します。



5. エラーの情報を使用して問題を修正してください。

   問題を解決すると、次回レポートを実行したときにエラーは表示されなくなります。

レポートを削除する

修正したエラーが含まれているレポートや、削除した同期関係に関連したレポートを削除することがあります。

手順

1. *同期 > レポート*を選択します。
2. レポート アクション 列で、パスのアクション メニューを選択し、最後のレポートを削除 または すべてのレポートを削除 を選択します。
3. レポートを削除することを確認します。

NetApp Copy and Syncのデータブローカーをアンインストールする

必要に応じて、アンインストール スクリプトを実行して、データ ブローカーと、データ ブローカーのインストール時にNetApp Copy and Sync用に作成されたパッケージおよびディレクトリを削除します。

手順

1. データ ブローカー ホストにログインします。
2. データ ブローカー ディレクトリに変更します。 `/opt/netapp/databroker`
3. 次のコマンドを実行します。

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

4. アンインストールを確認するには「y」を押します。

NetApp Copy and SyncAPI

Web UI を通じて利用できるNetApp Copy and Sync機能は、RESTful API を通じても利用できます。

始めましょう

コピーおよび同期 API の使用を開始するには、ユーザー トークンとNetApp Consoleアカウント ID を取得する必要があります。 API 呼び出しを行うときは、トークンとアカウント ID を Authorization ヘッダーに追加する必要があります。

手順

1. NetApp Consoleからユーザー トークンを取得します。

```
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>"
}
```

クライアント ID のない個人のメール アカウントを使用している場合は、デフォルトのクライアント ID「QC3AgHk6qdbmC7Yyr82ApBwaaJLwRrNO」を使用できます。

2. NetApp Consoleアカウント ID を取得します。

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

この API は次のような応答を返します。

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

3. 各 API 呼び出しの Authorization ヘッダーにユーザー トークンとアカウント ID を追加します。

   例

   次の例は、Microsoft Azure でデータ ブローカーを作成するための API 呼び出しを示しています。<user_token> と <accountId> を、前の手順で取得したトークンと ID に置き換えるだけです。

```
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" }
```

次の手順

NetApp Consoleからのユーザー トークンには有効期限があります。トークンを更新するには、手順 1 から API を再度呼び出す必要があります。

API レスポンスには、トークンの有効期限を示す「expires_in」フィールドが含まれています。

リストAPIを使用する

リスト API は非同期 API なので、結果はすぐに返されません (例: `GET /data-brokers/{id}/list-nfs-export-folders`そして `GET /data-brokers/{id}/list-s3-buckets`）。サーバーからの応答は HTTP ステータス 202 のみです。実際の結果を得るには、 `GET /messages/client` API。

手順

1. 使用したいリスト API を呼び出します。
2. 使用 `GET /messages/client`操作の結果を表示するための API。
3. 先ほど受け取った ID を追加して同じ API を使用します。 `GET http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   IDは呼び出すたびに変わるので注意してください。 `GET /messages/client` API。

例

電話すると `list-s3-buckets`API では、結果がすぐに返されません。

```
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>
```

結果は HTTP ステータス コード 202 です。これは、メッセージは受け入れられましたが、まだ処理されていないことを意味します。

操作の結果を取得するには、次の API を使用する必要があります。

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

結果は、ID フィールドを含む 1 つのオブジェクトを含む配列です。 ID フィールドは、サーバーが送信した最後のメッセージを表します。例えば：

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

受け取った ID を使用して、次の API 呼び出しを実行します。

```
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>
```

結果はメッセージの配列になります。各メッセージ内にはペイロード オブジェクトが含まれており、これは操作の名前 (キー) とその結果 (値) で構成されます。例えば：

```
[
    {
        "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リファレンス

各コピーおよび同期APIのドキュメントは以下から入手できます。 https://api.cloudsync.netapp.com/docs 。

概念

NetApp Copy and Syncのライセンスの概要

14 日間の無料トライアルが終了した後、 NetApp Copy and Sync関係の支払い方法は 2 つあります。最初のオプションは、AWS または Azure から従量課金制または年間払いでサブスクライブすることです。 2 番目のオプションは、 NetAppから直接ライセンスを購入することです。

ライセンスは、 NetApp Consoleではなく、 NetApp Copy and Syncまたは該当する Web サイトを通じて管理する必要があります。

マーケットプレイスサブスクリプション

AWS または Azure からのコピーと同期をサブスクライブすると、時間単位で支払うことも、年単位で支払うこともできます。"AWSまたはAzureを通じてサブスクライブできます"請求先に応じて異なります。

> コピーと同期は、**AWS** と **Azure** からの Marketplace サブスクリプションのみをサポートします。Google Cloud Marketplace サブスクリプションは、コピーと同期ではサポートされていません。

時間単位のサブスクリプション

時間単位の従量課金制サブスクリプションでは、作成した同期関係の数に基づいて時間ごとに課金されます。

- "Azure の価格を見る"
- "AWS の従量課金制料金を見る"

年間購読

年間サブスクリプションでは、前払いで支払う 20 の同期関係のライセンスが提供されます。同期関係が 20 を超え、AWS を通じてサブスクライブしている場合は、追加の関係に対して時間単位で料金が発生します。

"AWSの年間料金を見る"

NetAppのライセンス

同期関係の料金を前払いする別の方法は、 NetAppから直接ライセンスを購入することです。各ライセンスでは、最大 20 個の同期関係を作成できます。

これらのライセンスは、AWS または Azure サブスクリプションで使用できます。たとえば、同期関係が 25 個ある場合、ライセンスを使用して最初の 20 個の同期関係に対して料金を支払い、残りの 5 個の同期関係については AWS または Azure から従量課金制で支払うことができます。

"ライセンスを購入してNetApp Copy and Syncに追加する方法について学びます" 。

ライセンス条項

コピーおよび同期のために Bring Your Own License (BYOL) を購入するお客様は、ライセンス資格に関連する制限事項に注意する必要があります。

- お客様は、納品日から 1 年を超えない期間、BYOL ライセンスを活用する権利を有します。
- お客様は、BYOL ライセンスを活用して、ソースとターゲット間の個別の接続 (それぞれ「同期関係」) を合計 20 個まで確立することができます。
- お客様が 20 の同期関係の制限に達したかどうかに関係なく、お客様の権利は 1 年間のライセンス期間の終了時に失効します。
- お客様がライセンスの更新を選択した場合、以前のライセンス付与に関連付けられた未使用の同期関係はライセンスの更新に引き継がれません。

NetApp Copy and Syncにおけるデータプライバシー

NetApp は、NetApp Copy and Syncの使用中に提供された資格情報にアクセスできません。資格情報は、ネットワーク内にあるデータ ブローカー マシンに直接保存されます。

選択した構成によっては、新しい関係を作成するときに、コピーと同期によって資格情報の入力が求められる場合があります。たとえば、SMB サーバーを含む関係を設定する場合や、AWS にデータブローカーをデプロイする場合などです。

これらの資格情報は常にデータ ブローカー自体に直接保存されます。データ ブローカーは、オンプレミスでもクラウド アカウントでも、ネットワーク内のマシンに存在します。資格情報はNetAppに提供されることはありません。

資格情報は、HashiCorp Vault を使用してデータ ブローカー マシン上でローカルに暗号化されます。

NetApp Copy and Sync技術 FAQ

質問に対する簡単な回答を探している場合は、この FAQ が役立ちます。

開始

次の質問は、NetApp Copy and Syncの使用開始に関連しています。

NetApp Copy and Sync はどのように機能しますか**?**

コピーと同期では、 NetAppデータ ブローカー ソフトウェアを使用して、ソースからターゲットにデータを同期します (これを 同期関係 と呼びます)。

データ ブローカー グループは、ソースとターゲット間の同期関係を制御します。同期関係を設定すると、コピーと同期によってソース システムを分析し、複数のレプリケーション ストリームに分割して、選択したターゲット データにプッシュします。

最初のコピーの後、コピーと同期は設定したスケジュールに基づいて変更されたデータを同期します。

14 日間の無料トライアルはどのように機能しますか?

14 日間の無料トライアルは、Copy and Sync にサインアップすると開始されます。作成したコピーおよび同期関係に対しては、14 日間NetApp の料金は発生しません。ただし、デプロイするデータ ブローカーのすべてのリソース料金は引き続き適用されます。

コピーと同期にはいくらかかりますか?

コピーと同期の使用に関連するコストには、サービス料金とリソース料金の 2 種類があります。

サービス料

従量課金制の場合、コピーおよび同期サービスの料金は、作成する同期関係の数に基づいて時間単位で課金されます。

- "AWS の従量課金制料金を見る"
- "AWSの年間料金を見る"
- "Azure の価格を見る"

コピー ライセンスと同期ライセンスは、 NetApp担当者を通じても入手できます。各ライセンスでは、12 か月間に 20 の同期関係が有効になります。

"ライセンスについて詳しくはこちら" 。

コピーおよび同期関係は、Azure NetApp Filesでは無料です。

リソース料金

リソース料金は、クラウドでデータ ブローカーを実行するためのコンピューティング コストとストレージ コストに関連しています。

コピーと同期はどのように請求され、サブスクリプションはどのように管理すればよいですか?

14 日間の無料トライアルが終了した後、同期関係の料金を支払う方法は 2 つあります。最初のオプションは、AWS または Azure からサブスクライブすることです。これにより、従量課金制または年間支払いが可能になります。 2 番目のオプションは、 NetAppから直接ライセンスを購入することです。いずれの場合も、サブスクリプションは、コピーと同期のユーザー インターフェースではなく、プロバイダー マーケットプレイスを通じて管理されます。

クラウド外でもコピーと同期を使用できますか?

はい、非クラウド アーキテクチャでもコピーと同期を使用できます。ソースとターゲットはオンプレミスに存在でき、データ ブローカー ソフトウェアも同様にオンプレミスに存在できます。

クラウド外でコピーと同期を使用する場合は、次の重要な点に注意してください。

- データ ブローカー グループは、コピーおよび同期と通信するためにインターネット接続が必要です。
- NetAppから直接ライセンスを購入しない場合は、PAYGO コピーおよび同期の課金のために AWS または Azure アカウントが必要になります。

コピーと同期にアクセスするにはどうすればよいですか?

コピーと同期はNetApp Consoleから利用できます。コンソールの左側のナビゲーションから、モビリティ > *コピーと同期*を選択します。

データ ブローカー グループとは何ですか?

各データ ブローカーはデータ ブローカー グループに属します。データ ブローカーをグループ化すると、同期関係のパフォーマンスが向上します。

サポートされているソースとターゲット

次の質問は、同期関係でサポートされるソースとターゲットに関連しています。

コピーと同期はどのソースとターゲットをサポートしていますか?

コピーと同期は、さまざまな種類の同期関係をサポートします。"リスト全体を見る" 。

コピーと同期はどのバージョンの **NFS** と **SMB** をサポートしていますか?

コピーと同期は、NFS バージョン 3 以降と SMB バージョン 1 以降をサポートしています。

"同期要件の詳細" 。

Amazon S3 がターゲットの場合、データを特定の **S3** ストレージクラスに階層化できますか?

はい、AWS S3 がターゲットの場合は、特定の S3 ストレージ クラスを選択できます。

- 標準（これがデフォルトのクラスです）
- インテリジェントティアリング
- 標準-低頻度アクセス
- 1つのゾーン - 低頻度アクセス
- グレイシャーディープアーカイブ
- 氷河フレキシブルリトリーバル
- 氷河の即時検索

Azure Blob ストレージのストレージ層はどうですか?

BLOB コンテナーがターゲットの場合は、特定の Azure BLOB ストレージ層を選択できます。

- ホットストレージ
- クールストレージ

Google Cloud のストレージ階層をサポートしていますか?

はい、Google Cloud Storage バケットがターゲットの場合は、特定のストレージ クラスを選択できます。

- Standard

- ニアライン
- コールドライン
- アーカイブ

ネットワーク

次の質問は、コピーと同期のネットワーク要件に関連しています。

コピーと同期のネットワーク要件は何ですか?

コピーおよび同期環境では、データ ブローカー グループが、選択したプロトコルまたはオブジェクト ストレージ API (Amazon S3、Azure Blob、IBM Cloud Object Storage) を介してソースおよびターゲットに接続されている必要があります。

さらに、データ ブローカー グループには、Copy and Sync と通信し、他のいくつかのサービスやリポジトリに接続できるように、ポート 443 経由の送信インターネット接続が必要です。

詳細については、"ネットワーク要件を確認する" 。

データ ブローカーでプロキシ サーバーを使用できますか?

○

コピーと同期は、基本認証の有無にかかわらずプロキシ サーバーをサポートします。データ ブローカーをデプロイするときにプロキシ サーバーを指定すると、データ ブローカーからのすべての HTTP および HTTPS トラフィックはプロキシ経由でルーティングされます。 NFS や SMB などの非 HTTP トラフィックはプロキシ サーバー経由でルーティングできないことに注意してください。

プロキシ サーバーの唯一の制限は、NFS またはAzure NetApp Files の同期関係でデータインフライト暗号化を使用する場合です。暗号化されたデータは HTTPS 経由で送信され、プロキシ サーバー経由でルーティングすることはできません。

データ同期

次の質問は、データ同期の仕組みに関するものです。

同期はどのくらいの頻度で行われますか?

デフォルトのスケジュールは毎日同期するように設定されています。最初の同期後に、次の操作を実行できます。

- 同期スケジュールを希望の日数、時間、分数に変更します
- 同期スケジュールを無効にする
- 同期スケジュールを削除します（データは失われず、同期関係のみが削除されます）

最小同期スケジュールは何ですか?

関係を 1 分ごとに同期するようにスケジュールできます。

ファイルの同期に失敗した場合、データ ブローカー グループは再試行しますか? それともタイムアウトになりますか?

1 つのファイルの転送に失敗しても、データ ブローカー グループはタイムアウトしません。代わりに、データ ブローカー グループは、ファイルをスキップする前に 3 回再試行します。再試行値は、同期関係の設定で構成できます。

"同期関係の設定を変更する方法を学ぶ" 。

データセットが非常に大きい場合はどうすればよいですか?

1つのディレクトリに600,000以上のファイルが含まれている場合、"お問い合わせ"ペイロードを処理するためのデータ ブローカー グループの構成を支援できるようになります。データ ブローカー グループに追加のメモリを追加する必要がある可能性があります。

マウント ポイント内のファイルの総数には制限がないことに注意してください。階層のレベル (最上位ディレクトリまたはサブディレクトリ) に関係なく、600,000 個以上のファイルを含む大規模なディレクトリには追加のメモリが必要です。

セキュリティ

以下の質問はセキュリティに関するものです。

コピーと同期は安全ですか?

○すべてのコピーと同期のネットワーク接続は、 "Amazon シンプルキューサービス (SQS)" 。

データブローカー グループと Amazon S3、Azure Blob、Google Cloud Storage、IBM Cloud Object Storage 間のすべての通信は、HTTPS プロトコルを介して行われます。

オンプレミス (ソースまたは宛先) システムでコピーと同期を使用している場合は、次の接続オプションが推奨されます。

- インターネットを経由しないルーティング（指定したクラウド ネットワークとのみ通信可能）である AWS Direct Connect、Azure ExpressRoute、または Google Cloud Interconnect 接続
- オンプレミスのゲートウェイデバイスとクラウドネットワーク間のVPN接続
- S3 バケット、Azure Blob ストレージ、または Google Cloud Storage を使用したデータ転送の安全性をさらに高めるには、Amazon プライベート S3 エンドポイント、Azure 仮想ネットワーク サービス エンドポイント、またはプライベート Google アクセスを確立できます。

これらの方法はいずれも、オンプレミスの NAS サーバーとコピーおよび同期データ ブローカー グループ間の安全な接続を確立します。

コピーと同期によってデータは暗号化されますか?

- コピーと同期は、ソース NFS サーバーとターゲット NFS サーバー間のデータインフライト暗号化をサポートします。"詳細情報" 。
- SMB の場合、コピーと同期は、サーバー側で暗号化された SMB 3.0 および 3.11 データをサポートします。コピーと同期は、暗号化されたデータをソースからターゲットにコピーし、データは暗号化されたままになります。

コピーと同期では、SMB データ自体を暗号化することはできません。

- Amazon S3 バケットが同期関係のターゲットである場合、AWS KMS 暗号化または AES-256 暗号化を使用してデータ暗号化を有効にするかどうかを選択できます。
- Google ストレージ バケットが同期関係のターゲットである場合、デフォルトの Google 管理の暗号化キーを使用するか、独自の KMS キーを使用するかを選択できます。

権限

次の質問はデータの権限に関するものです。

SMB データ権限はターゲットの場所に同期されていますか**?**

コピーと同期を設定すると、ソース SMB 共有とターゲット SMB 共有間、およびソース SMB 共有からオブジェクト ストレージ (ONTAP S3 を除く) へのアクセス制御リスト (ACL) を保持できます。

コピーと同期では、オブジェクト ストレージから SMB 共有への ACL のコピーはサポートされていません。

"SMB共有間でACLをコピーする方法を学ぶ" 。

Copy Sync は SMB ACL (アクセス許可) をコピーしますが、ファイルまたはフォルダーの所有権はコピーしません。所有権属性は、SMB ACL コピー操作には含まれません。 SMB共有間でデータをコピーする際に所有権を保持する必要がある場合は、 `robocopy`セキュリティ情報を手動でコピーします。例えば、 `/copyall`フラグは ACL、所有者、監査データをコピーします。

NFS データの権限はターゲットの場所に同期されていますか**?**

コピーと同期は、次のように NFS サーバー間で NFS 権限を自動的にコピーします。

- NFS バージョン 3: コピーと同期は、権限とユーザー グループの所有者をコピーします。
- NFS バージョン 4: コピーと同期は ACL をコピーします。

オブジェクトストレージメタデータ

どのような同期関係がオブジェクト ストレージ メタデータを保存しますか**?**

コピーと同期は、次の種類の同期関係について、オブジェクト ストレージ メタデータをソースからターゲットにコピーします。

- Amazon S3 → Amazon S3 [1]
- Amazon S3 →StorageGRID
- StorageGRID→ Amazon S3
- StorageGRID→StorageGRID
- StorageGRID → Google Cloud Storage
- Google Cloud Storage → StorageGRID [1]
- Google Cloud Storage → IBM Cloud オブジェクト ストレージ [1]

- Google クラウド ストレージ → Amazon S3 [1]
- Amazon S3 → Google クラウド ストレージ
- IBM Cloud オブジェクト ストレージ → Google Cloud ストレージ
- StorageGRID → IBM Cloud オブジェクトストレージ
- IBM Cloud オブジェクトストレージ → StorageGRID
- IBM Cloud オブジェクト ストレージ → IBM Cloud オブジェクト ストレージ

[1] これらの同期関係では、"同期関係を作成するときにオブジェクトのコピー設定を有効にします" 。

NFS または **SMB** がソースである場合の同期中に、どのような種類のメタデータが複製されますか**?**

ユーザー ID、変更時刻、アクセス時刻、GID などのメタデータはデフォルトで複製されます。ユーザーは、同期関係を作成するときに ACL を必須としてマークすることにより、CIF から ACL を複製することを選択できます。

パフォーマンス

次の質問は、コピーと同期のパフォーマンスに関するものです。

同期関係の進行状況インジケーターは何を表していますか**?**

同期関係には、データ ブローカー グループのネットワーク アダプターのスループットが表示されます。複数のデータ ブローカーを使用して同期パフォーマンスを高速化した場合、スループットはすべてのトラフィックの合計になります。このスループットは 20 秒ごとに更新されます。

パフォーマンスの問題が発生しています。同時転送の数を制限することはできますか**?**

ファイルが非常に大きい場合 (それぞれ複数 TiB)、転送プロセスの完了に長い時間がかかり、パフォーマンスに影響が出る可能性があります。

同時転送の数を制限すると役立ちます。"ヘルプが必要な場合はお問い合わせください" 。

Azure NetApp Filesのパフォーマンスが低下するのはなぜですか**?**

Azure NetApp Filesとの間でデータを同期する場合、ディスク サービス レベルが Standard の場合は障害やパフォーマンスの問題が発生する可能性があります。

同期パフォーマンスを向上させるには、サービス レベルを Premium または Ultra に変更します。

"Azure NetApp Files のサービス レベルとスループットの詳細" 。

グループには何人のデータ ブローカーが必要ですか**?**

新しい関係を作成するときは、グループ内の単一のデータ ブローカーから開始します (高速同期関係に属する既存のデータ ブローカーを選択した場合を除く)。多くの場合、単一のデータ ブローカーで同期関係のパフォーマンス要件を満たすことができます。そうでない場合は、グループにデータ ブローカーを追加することで同期のパフォーマンスを向上できます。ただし、まず同期パフォーマンスに影響を与える可能性のある他の要因を確認する必要があります。

データ転送のパフォーマンスには複数の要因が影響する可能性があります。全体的な同期パフォーマンスは、ネットワーク帯域幅、待ち時間、ネットワーク トポロジ、およびデータ ブローカー VM の仕様とストレージ システムのパフォーマンスによって影響を受ける可能性があります。たとえば、グループ内の単一のデータ ブローカーは 100 MB/秒に到達できますが、ターゲットのディスク スループットは 64 MB/秒しか許可されない場合があります。その結果、データ ブローカー グループはデータのコピーを試行し続けますが、ターゲットはデータ ブローカー グループのパフォーマンスを満たすことができません。

したがって、ネットワークのパフォーマンスとターゲット上のディスク スループットを必ず確認してください。

次に、グループにデータ ブローカーを追加してその関係の負荷を分散し、同期パフォーマンスを高速化することを検討できます。"同期パフォーマンスを高速化する方法を学ぶ" 。

削除する

次の質問は、ソースとターゲットから同期関係とデータを削除することに関するものです。

コピーと同期の関係を削除するとどうなりますか?

関係を削除すると、今後のすべてのデータ同期が停止され、支払いが終了します。ターゲットに同期されたデータはそのまま残ります。

ソースサーバーから何かを削除するとどうなりますか? ターゲットからも削除されますか?

デフォルトでは、アクティブな同期関係がある場合、ソース サーバーで削除された項目は、次回の同期時にターゲットから削除されません。ただし、各関係の同期設定にはオプションがあり、ソースからファイルが削除された場合にコピーと同期によってターゲットの場所にあるファイルも削除するように定義できます。

"同期関係の設定を変更する方法を学ぶ" 。

ターゲットから何かを削除するとどうなりますか? 私のソースからも削除されましたか?

アイテムがターゲットから削除されても、ソースからは削除されません。関係はソースからターゲットへの一方向です。次の同期サイクルでは、コピーと同期によってソースとターゲットが比較され、アイテムが不足していることが識別され、コピーと同期によってそのアイテムがソースからターゲットに再度コピーされます。

トラブルシューティング

"NetAppナレッジベース: コピーと同期に関する FAQ: サポートとトラブルシューティング"

データブローカーの詳細

次の質問はデータ ブローカーに関するものです。

データブローカーのアーキテクチャについて説明していただけますか?

もちろん。最も重要なポイントは次のとおりです。

- データ ブローカーは、Linux ホスト上で実行される node.js アプリケーションです。
- コピーと同期は、データ ブローカーを次のように展開します。

- AWS: AWS CloudFormation テンプレートから
- Azure: Azure リソース マネージャーから
- Google: Google Cloud Deployment Manager から
- 独自のLinuxホストを使用する場合は、ソフトウェアを手動でインストールする必要があります。

- データ ブローカー ソフトウェアは自動的に最新バージョンにアップグレードされます。
- データブローカーは、信頼性が高く安全な通信チャネルとして、また制御と監視のために AWS SQS を使用します。 SQS は永続性レイヤーも提供します。
- 転送速度を向上させ、高可用性を高めるために、グループにデータ ブローカーを追加できます。 1 つのデータ ブローカーに障害が発生した場合でも、サービスの回復力は確保されます。

知識とサポート

サポートに登録する

NetApp Consoleとそのストレージ ソリューションおよびデータ サービスに固有のテクニカル サポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウド プロバイダー ファイル サービスに対するNetAppサポートは有効になりません。クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のドキュメントの「ヘルプの取得」を参照してください。

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

サポート登録の概要

サポート資格を有効にするには、次の 2 つの登録形式があります。

- NetApp Consoleアカウントのシリアル番号 (コンソールの [サポート リソース] ページにある 20 桁の 960xxxxxxxxx シリアル番号) を登録します。

  これは、コンソール内のすべてのサービスに対する単一のサポート サブスクリプション ID として機能します。各コンソール アカウントを登録する必要があります。

- クラウド プロバイダーのマーケットプレイスで、サブスクリプションに関連付けられたCloud Volumes ONTAPシリアル番号を登録します (これらは 20 桁の 909201xxxxxxxx シリアル番号です)。

  これらのシリアル番号は一般に *PAYGO* シリアル番号 と呼ばれ、 Cloud Volumes ONTAP の導入時にNetApp Consoleによって生成されます。

両方のタイプのシリアル番号を登録すると、サポート チケットの開設やケースの自動生成などの機能が有効になります。登録は、以下の説明に従ってNetAppサポート サイト (NSS) アカウントをコンソールに追加することで完了します。

NetAppサポートのためにNetApp Consoleを登録する

サポートに登録し、サポート資格を有効にするには、 NetApp Consoleアカウントの 1 人のユーザーがNetAppサポート サイト アカウントをコンソール ログインに関連付ける必要があります。NetAppサポートに登録する方法は、 NetAppサポート サイト (NSS) アカウントをすでにお持ちかどうかによって異なります。

NSSアカウントをお持ちの既存顧客

NSS アカウントをお持ちのNetApp のお客様の場合は、コンソールからサポートに登録するだけです。

手順

1. 管理 > *資格情報*を選択します。
2. *ユーザー資格情報*を選択します。
3. **NSS** 資格情報の追加 を選択し、 NetAppサポート サイト (NSS) の認証プロンプトに従います。
4. 登録プロセスが成功したことを確認するには、[ヘルプ] アイコンを選択し、[サポート] を選択します。

   リソース ページには、コンソール アカウントがサポートに登録されていることが表示されます。

   他のコンソール ユーザーは、ログインにNetAppサポート サイト アカウントを関連づけていない場合、同じサポート登録ステータスを表示しないことに注意してください。ただし、これはあなたのアカウントがサポートに登録されていないことを意味するものではありません。組織内の 1 人のユーザーがこれらの手順を実行していれば、アカウントは登録済みになります。

既存の顧客だが**NSS**アカウントがない

既存のNetApp顧客であり、既存のライセンスとシリアル番号を持っているものの、NSS アカウントを持っていない場合は、NSS アカウントを作成し、それをコンソール ログインに関連付ける必要があります。

手順

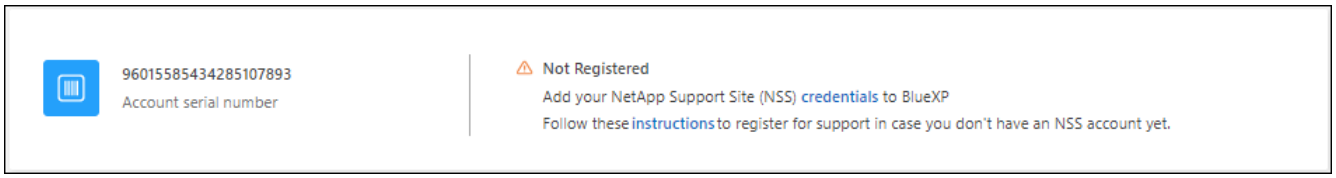
1. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したコンソール アカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより、アカウント処理が高速化されます。
2. 以下の手順を実行して、新しいNSSアカウントをコンソールログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

NetAppの新着情報

NetAppを初めて使用し、NSS アカウントをお持ちでない場合は、以下の手順に従ってください。

手順

1. コンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。
2. サポート登録ページからアカウント ID シリアル番号を見つけます。



3. 移動先 "NetAppのサポート登録サイト"私は登録済みの**NetApp**顧客ではありません を選択します。
4. 必須フィールド（赤いアスタリスクが付いているフィールド）に入力します。
5. 製品ライン フィールドで、**Cloud Manager** を選択し、該当する請求プロバイダーを選択します。
6. 上記の手順 2 からアカウントのシリアル番号をコピーし、セキュリティ チェックを完了して、NetApp のグローバル データ プライバシー ポリシーを読んだことを確認します。

   この安全な取引を完了するために、指定されたメールボックスに電子メールが直ちに送信されます。検証

メールが数分以内に届かない場合は、必ずスパム フォルダーを確認してください。

7. メール内からアクションを確認します。

   確認すると、リクエストがNetAppに送信され、 NetAppサポート サイトのアカウントを作成することが推奨されます。

8. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより処理速度が向上します。

終了後の操作

このプロセス中に、 NetAppから連絡が来るはずです。これは、新規ユーザー向けの 1 回限りのオンボーディング演習です。

NetAppサポートサイトのアカウントを取得したら、以下の手順を実行して、アカウントをコンソールログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける

Cloud Volumes ONTAPの次の主要なワークフローを有効にするには、 NetAppサポート サイトの認証情報をコンソール アカウントに関連付ける必要があります。

- 従量課金制のCloud Volumes ONTAPシステムをサポート対象として登録する

  システムのサポートを有効にし、 NetAppテクニカル サポート リソースにアクセスするには、NSS アカウントを提供する必要があります。

- BYOL（個人ライセンス使用）時にCloud Volumes ONTAP を導入する

  コンソールがライセンス キーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSS アカウントを提供する必要があります。これには、期間更新の自動更新が含まれます。

- Cloud Volumes ONTAPソフトウェアを最新リリースにアップグレードする

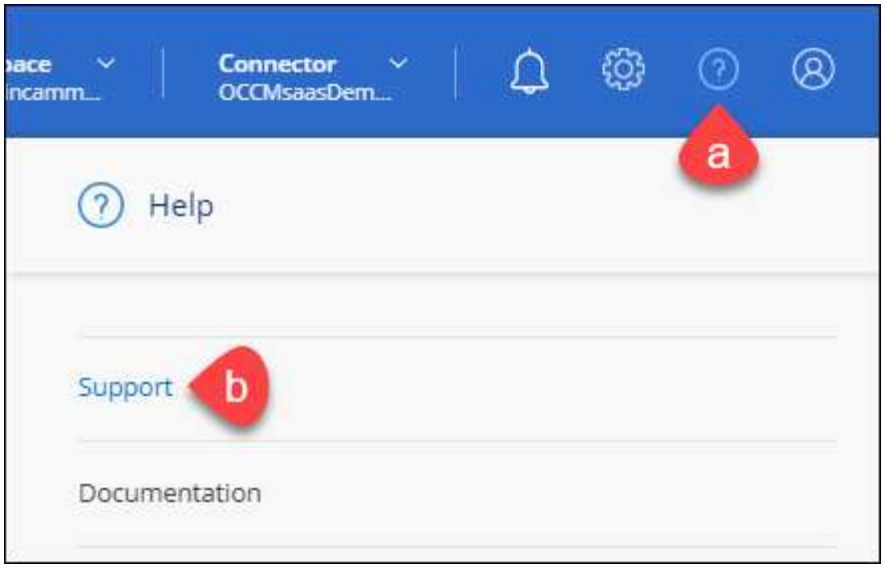
NSS 資格情報をNetApp Consoleアカウントに関連付けることは、コンソール ユーザー ログインに関連付けられている NSS アカウントとは異なります。

これらの NSS 資格情報は、特定のコンソール アカウント ID に関連付けられています。コンソール組織に属するユーザーは、サポート **> NSS** 管理 からこれらの資格情報にアクセスできます。

- 顧客レベルのアカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できます。
- パートナー アカウントまたは再販業者アカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できますが、顧客レベルのアカウントと一緒に追加することはできません。

手順

1. コンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. *NSS管理 > NSSアカウントの追加*を選択します。
3. プロンプトが表示されたら、[続行] を選択して、Microsoft ログイン ページにリダイレクトします。

   NetApp は、サポートとライセンスに固有の認証サービスの ID プロバイダーとして Microsoft Entra ID を使用します。

4. ログイン ページで、 NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力して、認証プロセスを実行します。

   これらのアクションにより、コンソールはライセンスのダウンロード、ソフトウェア アップグレードの検証、将来のサポート登録などに NSS アカウントを使用できるようになります。

   次の点に注意してください。

   - NSS アカウントは顧客レベルのアカウントである必要があります (ゲスト アカウントや一時アカウントではありません)。顧客レベルの NSS アカウントを複数持つことができます。
   - パートナー レベルのアカウントの場合、NSS アカウントは 1 つだけ存在できます。顧客レベルの NSS アカウントを追加しようとしたときに、パートナー レベルのアカウントが存在する場合は、次のエラー メッセージが表示されます。

     「異なるタイプの NSS ユーザーがすでに存在するため、このアカウントでは NSS 顧客タイプは許可されません。」

   既存の顧客レベルの NSS アカウントがあり、パートナー レベルのアカウントを追加しようとする場合も同様です。

   - ログインが成功すると、 NetApp はNSS ユーザー名を保存します。

     これは、メールにマッピングされるシステム生成の ID です。*NSS管理*ページでは、 ••• メニュー。

   - ログイン認証トークンを更新する必要がある場合は、 ••• メニュー。

     このオプションを使用すると、再度ログインするよう求められます。これらのアカウントのトークンは 90 日後に期限切れになることに注意してください。これを知らせる通知が投稿されます。

ヘルプを受ける

NetAppは、 BlueXPとそのクラウドサービスに対して、様々なサポートを提供しています。ナレッジベース（KB）記事やコミュニティフォーラムなど、充実した無料のセルフサポートオプションを24時間365日ご利用いただけます。サポート登録には、Webチケットによるリモートテクニカルサポートも含まれます。

クラウドプロバイダーのファイルサービスのサポートを受ける

クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のBlueXPドキュメントの「ヘルプの取得」を参照してください。

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

BlueXPとそのストレージ ソリューションおよびサービスに固有のテクニカル サポートを受けるには、以下に説明するサポート オプションを使用してください。

セルフサポートオプションを使用する

以下のオプションは、24 時間 365 日無料でご利用いただけます。

- ドキュメント

  現在表示しているBlueXPドキュメント。

- "ナレッジベース"

  BlueXPナレッジベースを検索して、問題のトラブルシューティングに役立つ記事を見つけます。

- "コミュニティ"

  BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりしてください。

NetAppサポートでケースを作成する

上記のセルフ サポート オプションに加えて、サポートを有効にした後は、 NetAppサポート スペシャリストと協力して問題を解決することもできます。

始める前に

- *ケースの作成*機能を使用するには、まずNetAppサポート サイトの資格情報をBlueXPログインに関連付ける必要があります。 "BlueXPログインに関連付けられた資格情報を管理する方法を学びます" 。
- シリアル番号を持つONTAPシステムのケースを開く場合は、NSS アカウントがそのシステムのシリアル番号に関連付けられている必要があります。

手順

1. BlueXPで、*ヘルプ > サポート*を選択します。
2. *リソース*ページで、テクニカル サポートの下にある利用可能なオプションのいずれかを選択します。

   a. 電話で誰かと話したい場合は、「電話する」を選択してください。電話をかけることができる電話番号をリストした netapp.com のページに移動します。

   b. NetAppサポート スペシャリストとのチケットを開くには、[ケースを作成] を選択します。

      - サービス: 問題が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能に関するテクニカル サポートの問題に固有の場合はBlueXP。
      - 作業環境: ストレージに該当する場合は、* Cloud Volumes ONTAP* または * On-Prem* を選択し、関連する作業環境を選択します。

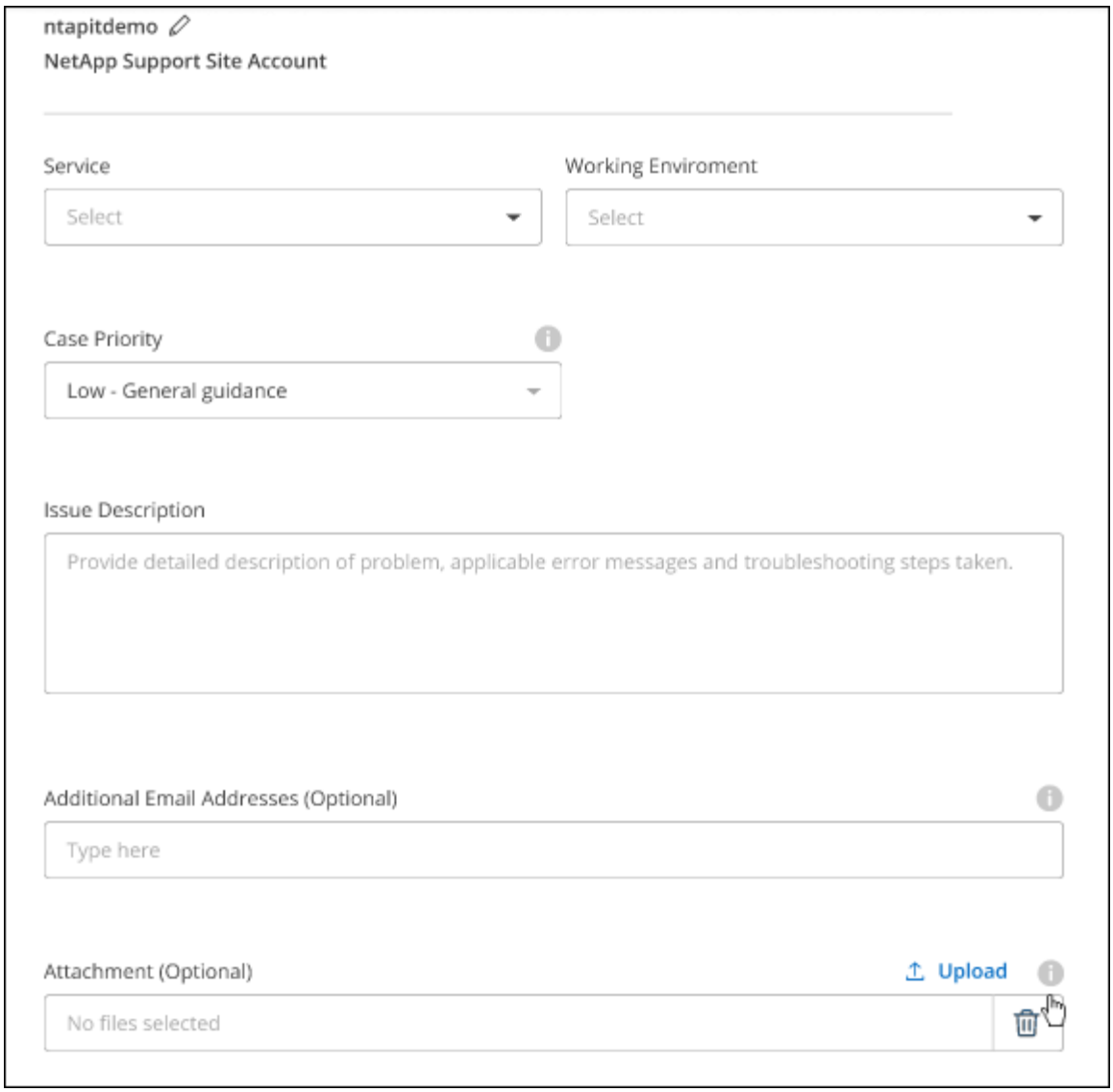
        作業環境のリストは、サービスのトップバナーで選択したBlueXP組織 (またはアカウント)、プロジェクト (またはワークスペース)、およびコネクタの範囲内にあります。

      - ケースの優先度: ケースの優先度 (低、中、高、重大) を選択します。

        これらの優先順位の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスを置きます。

      - 問題の説明: 該当するエラー メッセージや実行したトラブルシューティング手順など、問題の詳細な説明を入力します。
      - 追加のメールアドレス:この問題を他の人に知らせたい場合は、追加のメールアドレスを入力してください。
      - 添付ファイル **(**オプション**)**: 一度に 1 つずつ、最大 5 つの添付ファイルをアップロードします。

        添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。



終了後の操作

サポート ケース番号を示すポップアップが表示されます。NetAppサポート スペシャリストがお客様のケースを確認し、すぐにご連絡いたします。

サポート ケースの履歴については、設定 > タイムライン を選択し、「サポート ケースの作成」というアクションを探します。右端のボタンを使用すると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラー メッセージが表示される場合があります。

「選択したサービスに対してケースを作成する権限がありません」

このエラーは、NSS アカウントとそれに関連付けられているレコード会社が、 BlueXPアカウントのシリアル番号のレコード会社と同じではないことを意味している可能性があります (つまり、960xxxx) または作業環境のシリアル番号。次のいずれかのオプションを使用してサポートを求めることができます。

- 製品内チャットを使用する
- 非技術的なケースを提出する https://mysupport.netapp.com/site/help

サポートケースを管理する（プレビュー）

アクティブおよび解決済みのサポート ケースをBlueXPから直接表示および管理できます。NSS アカウントおよび会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして利用できます。今後のリリースでは、このエクスペリエンスを改良し、機能強化を追加する予定です。製品内チャットを使用してフィードバックをお送りください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の 2 つのビューがあります。
  - 左側のビューには、指定したユーザー NSS アカウントによって過去 3 か月間に開かれたケースの合計が表示されます。
  - 右側のビューには、ユーザーの NSS アカウントに基づいて、会社レベルで過去 3 か月間に開かれたケースの合計が表示されます。

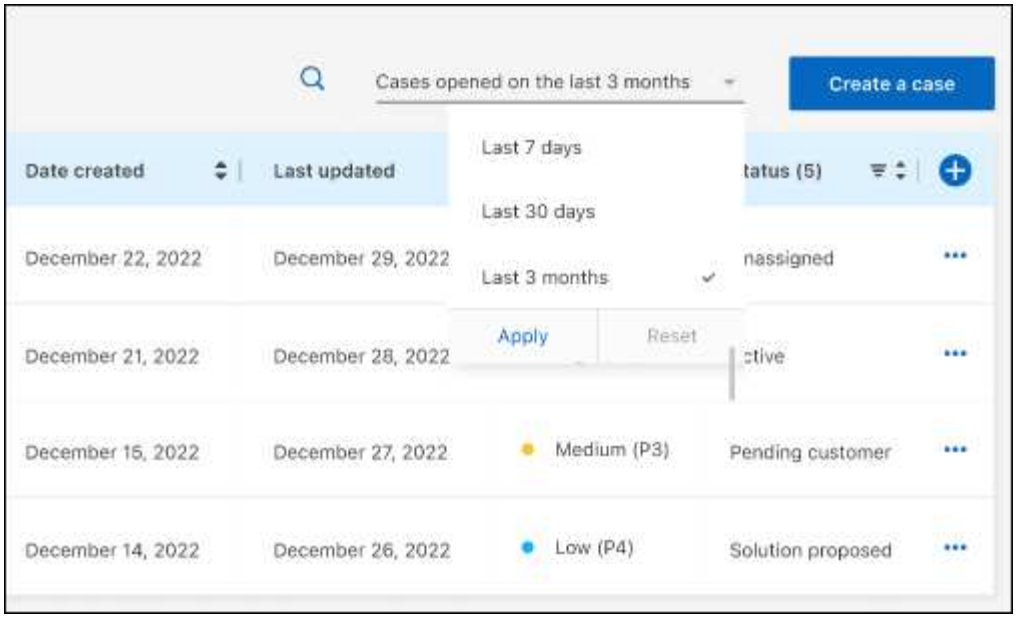
  表の結果には、選択したビューに関連するケースが反映されます。
- 関心のある列を追加または削除したり、優先度やステータスなどの列の内容をフィルタリングしたりできます。その他の列は並べ替え機能のみを提供します。

  詳細については、以下の手順をご覧ください。
- ケースごとに、ケースメモを更新したり、まだ「クローズ」または「クローズ保留中」ステータスになっていないケースをクローズしたりする機能を提供します。

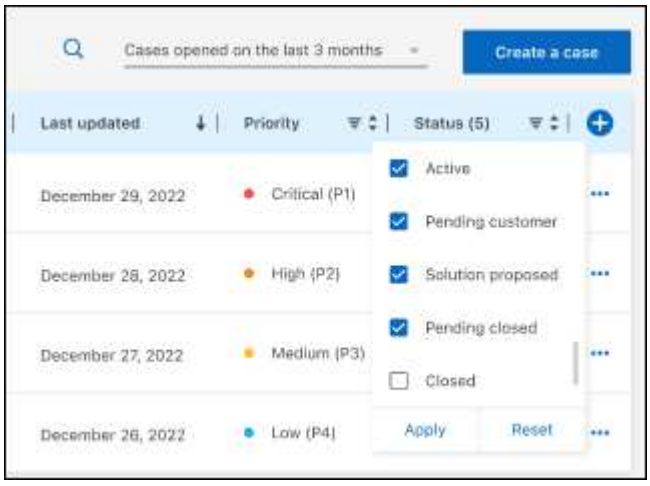
手順

1. BlueXPで、*ヘルプ > サポート*を選択します。
2. *ケース管理*を選択し、プロンプトが表示されたら、NSS アカウントをBlueXPに追加します。

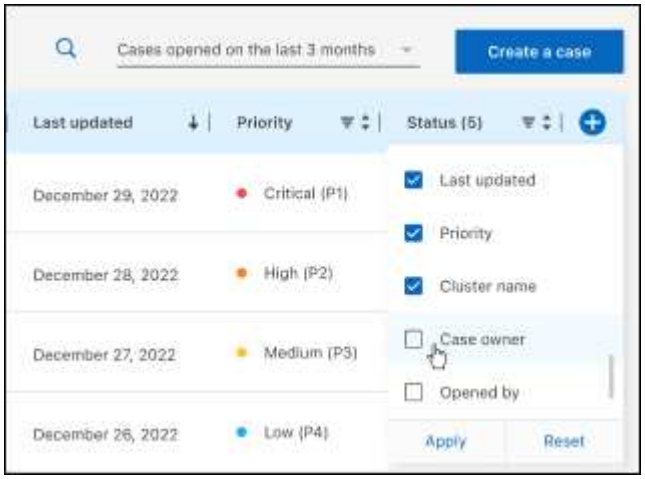
   ケース管理 ページには、 BlueXPユーザー アカウントに関連付けられている NSS アカウントに関連するオープン ケースが表示されます。これは、**NSS** 管理 ページの上部に表示される NSS アカウントと同じです。
3. 必要に応じて、テーブルに表示される情報を変更します。
   - *組織のケース*の下で*表示*を選択すると、会社に関連付けられているすべてのケースが表示されます。
   - 正確な日付範囲を選択するか、別の期間を選択して日付範囲を変更します。



◦ 列の内容をフィルタリングします。



◦ 表に表示される列を変更するには、次に、表示する列を選択します。

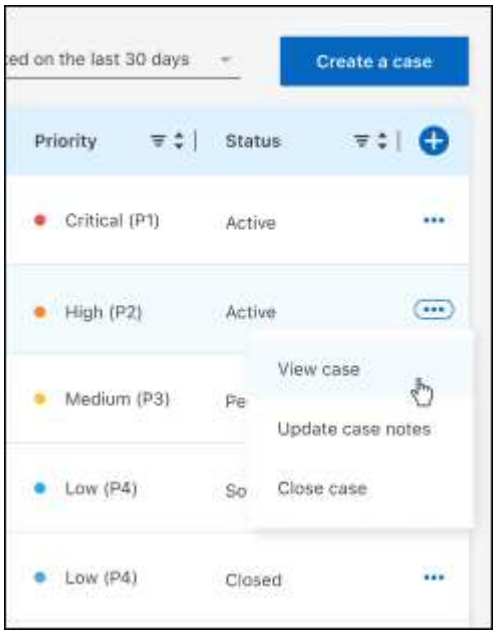


4. 既存のケースを管理するには、利用可能なオプションのいずれかを選択します。

- ケースを表示: 特定のケースに関する詳細をすべて表示します。
- ケースノートを更新: 問題に関する追加の詳細を入力するか、*ファイルのアップロード*を選択して最大 5 つのファイルを添付します。

  添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。

- ケースを閉じる: ケースを閉じる理由の詳細を入力し、[ケースを閉じる] を選択します。



法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシー ポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、 NetAppソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が提供されます。

"NetApp Copy and Syncに関するお知らせ"