



BlueXPのコピーと同期に関するドキュメント

BlueXP copy and sync

NetApp
April 08, 2024

目次

BlueXPのコピーと同期に関するドキュメント	1
リリースノート	2
BlueXPのコピーと同期の最新情報	2
制限	22
はじめに	24
BlueXPのコピーと同期の概要	24
BlueXPのコピーと同期のクイックスタート	26
サポートされている同期関係	27
ソースとターゲットを準備します	36
BlueXPのコピーと同期のネットワークの概要	43
データブローカーをインストール	47
BlueXPのコピーと同期を使用	65
ソースとターゲットの間でデータを同期します	65
無料トライアルの終了後に同期関係の料金を支払う	85
同期関係の管理	87
データブローカーグループの管理	94
レポートを作成および表示して、設定を調整します	101
データブローカーのアンインストール	105
BlueXPのコピーと同期のAPI	107
はじめに	107
API リファレンス	108
List API の使用	108
概念	111
ライセンスの概要	111
データのプライバシー	112
BlueXPのコピーと同期に関するテクニカルFAQ	112
知識とサポート	120
サポートに登録します	120
ヘルプを表示します	124
法的通知	130
著作権	130
商標	130
特許	130
プライバシーポリシー	130
オープンソース	130

BlueXPのコピーと同期に関するドキュメント

リリースノート

BlueXPのコピーと同期の最新情報

BlueXPのコピーと同期の新機能をご紹介します。

2024年4月8日

RHEL 8.9のサポート

データブローカーがRed Hat Enterprise Linux 8.9を実行するホストでサポートされるようになりました。

["Linuxホストの要件の表示"](#)。

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

ユーザはregex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*機能の詳細については、こちらを参照してください。"](#)

2023年11月26日

Azure Blobに対するコールドストレージクラスのサポート

同期関係の作成時にコールドストレージのAzure Blob階層を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は、こちらをご覧ください。"](#)

AWSデータブローカーでのTel Aviv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際に、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については、こちらをご覧ください。"](#)

データブローカーのノードバージョンの更新

これで、すべての新しいデータブローカーでノードバージョン21.2.0が使用されます。この更新プログラムと互換性のないデータブローカー（CentOS 7.0やUbuntu Server 18.0など）は、BlueXPのコピーと同期では使用できなくなります。

2023年9月3日

正規表現でファイルを除外

ユーザはregexを使用してファイルを除外するオプションを使用できるようになりました。

["*ファイル拡張子を除外*機能の詳細については、こちらをご覧ください。"](#)

Azureデータブローカー作成時にS3キーを追加

Azureデータブローカーの作成時にAWS S3のアクセスキーとシークレット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については、こちらをご覧ください。"](#)

2023年8月6日

データブローカーの作成時に既存の**Azure**セキュリティグループを使用する

データブローカーの作成時に既存のAzureセキュリティグループを使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/networkSecurityGroups/securityRules/read"
- Microsoft.Network/networkSecurityGroups/read"

["Azureでデータブローカーを作成する方法については、こちらをご覧ください。"](#)

Google Storageへの同期時にデータを暗号化する

Google Storageバケットをターゲットとする同期関係を作成するときに、ユーザが管理する暗号化キーを指定できるようになりました。キーは手動で入力することも、1つのリージョン内のキーのリストから選択することもできます。

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.list
- cloudkms.keyrings.list

["Google Cloud Storageバケットの要件については、こちらをご覧ください。"](#)

2023年7月9日

複数の同期関係を一度に削除

ユーザが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は、こちらを参照してください。"](#)

ACLのみをコピーします

CIF関係とNFS関係のACL情報をコピーするためのオプションが追加されました。同期関係を作成または管理する場合は、ファイルのみをコピー、ACL情報のみをコピー、ファイルとACL情報をコピーできます。

["ACLのコピーの詳細については、こちらをご覧ください。"](#)

Node.js 20に更新

コピーと同期がNode.js 20に更新されました。使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ません。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

分単位での自動中止をサポートします

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については、こちらを参照してください"](#)。

アクセス時間のメタデータをコピーします

ファイルシステムを含む関係では、* Copy for Objects *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。

["\[オブジェクトのコピー\]設定の詳細については、こちらを参照してください"\]](#)。

2023年5月8日

ハードリンク機能

セキュアでないNFSとNFSの関係を含む同期のハードリンクを含めることができるようになりました。

["ファイルタイプ設定の詳細については、こちらを参照してください"](#)。

セキュアな**NFS**関係にあるデータブローカーのユーザ証明書を追加できるようになりました

セキュアなNFS関係を作成する際に、ターゲットデータブローカー用に独自の証明書を設定できるようになりました。サーバ名を設定し、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使用できます。

最近変更されたファイルの除外期間が延長されました

スケジュールされた同期の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」設定の詳細については、こちらを参照してください"](#)。

UIで関係を関係IDでフィルタリングします

RESTful APIを使用するユーザは、関係IDを使用して関係をフィルタできるようになりました。

["BlueXPのコピーと同期でRESTful APIを使用する方法の詳細については、こちらをご覧ください"](#)。

["\[ディレクトリを除外する\]設定の詳細については、こちらを参照してください"\]](#)。

2023年4月2日

Azure Data Lake Storage Gen2関係のサポートが追加されました

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

- Azure NetApp Files の特長
- ONTAP 対応の Amazon FSX
- Cloud Volumes ONTAP
- On-Prem ONTAP の略

["サポートされている同期関係の詳細を確認できます"](#)。

完全パスでディレクトリをフィルタリングします

ディレクトリを名前でフィルタリングするだけでなく、完全パスで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。

["\[ディレクトリを除外する\]設定の詳細については、こちらを参照してください"](#)。

2023年3月7日

AWSデータブローカー向けの**EBS Encryption**

アカウントのKMSキーを使用して、AWSデータブローカーの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については、こちらをご覧ください"](#)。

2023年2月5日

Azure Data Lake Storage Gen2、**ONTAP S3**ストレージ、および**NFS**がサポートされるようになりました

Cloud Sync でONTAP S3ストレージおよびNFSの追加の同期関係がサポートされ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

Cloud Sync では、Azure Data Lake Storage Gen2もサポートしています。これは、以下の機能に対するソースとターゲットの両方に対応しています。

- NFS サーバ
- SMB サーバ
- ONTAP S3 ストレージ
- StorageGRID
- IBM クラウドオブジェクトストレージ

["サポートされている同期関係の詳細を確認できます"](#)。

Amazon Web Services データブローカーオペレーティングシステムにアップグレード

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に関する詳細を確認できます"](#)。

2023年1月3日

データブローカーのローカル設定を **UI** に表示します

ユーザが UI で各データブローカーのローカル設定を表示できるように、構成を表示*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に関する詳細情報"](#)。

Azure と **Google Cloud** データブローカーオペレーティングシステムにアップグレード

Azure と Google Cloud のデータブローカー向け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については、こちらをご覧ください"](#)。

["Google Cloud のデータブローカーインスタンスに関する詳細を確認できます"](#)。

2022年12月11日

ディレクトリを名前でフィルタリングします

同期関係に新しい*ディレクトリ名を除外*設定を使用できるようになりました。ユーザは、最大15個のディレクトリ名を同期から除外できます。デフォルトでは、.copy-Offload、.snapshot、~snapshot ディレクトリが除外されます。

["\[ディレクトリ名を除外する設定の詳細を確認してください\]"](#)。

Amazon S3 および **ONTAP S3** ストレージのサポートが追加されています

Cloud Sync で AWS S3 および ONTAP S3 ストレージの追加の同期関係がサポートされるようになりました。

- AWS S3 から ONTAP S3 ストレージ
- 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を確認できます"](#)。

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、ソースの 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。

Cloud Sync は、最初のデータ同期の完了後、ソースのAzureストレージバケットで変更をリスンし、ターゲットへの変更が発生した場合はその変更を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、およびStorageGRID に同期する場合に使用できます。

Azureデータブローカーでは、この設定を使用するためのカスタムロールと次の権限が必要です。

```
'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'
```

["Continuous Syncの詳細については、こちらをご覧ください"](#)。

2022年9月4日

Googleドライブの追加サポート

- Cloud Sync でGoogleドライブの同期関係が新たにサポートされるようになりました。
 - Google DriveからNFSサーバーへ
 - GoogleドライブからSMBサーバーへ
- Google Driveを含む同期関係に関するレポートを生成することもできます。

["レポートの詳細については、こちらをご覧ください"](#)。

継続的な同期機能の強化

次のタイプの同期関係で、継続的同期設定を有効にできるようになりました。

- NFSサーバへのS3バケット
- Google Cloud StorageをNFSサーバに接続している

["Continuous Syncの詳細については、こちらをご覧ください"](#)。

Eメール通知

Cloud Sync 通知をE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*Notification*設定を有効にしてから、BlueXPでAlerts and Notification設定を構成する必要があります。

["通知を設定する方法について説明します"](#)。

2022年7月31日

Googleドライブ

NFSサーバまたはSMBサーバからGoogle Drive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前に、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、こちらをご覧ください"](#)。

["サポートされている同期関係のリストを表示します"](#)。

Azure Data Lakeのサポートが追加されています

Cloud Sync で、Azure Data Lake Storage Gen2：

- Amazon S3からAzure Data Lake Storage Gen2への接続に対応しています
- IBM Cloud Object StorageからAzure Data Lake Storage Gen2への接続
- StorageGRID からAzureデータレイクストレージGen2への接続

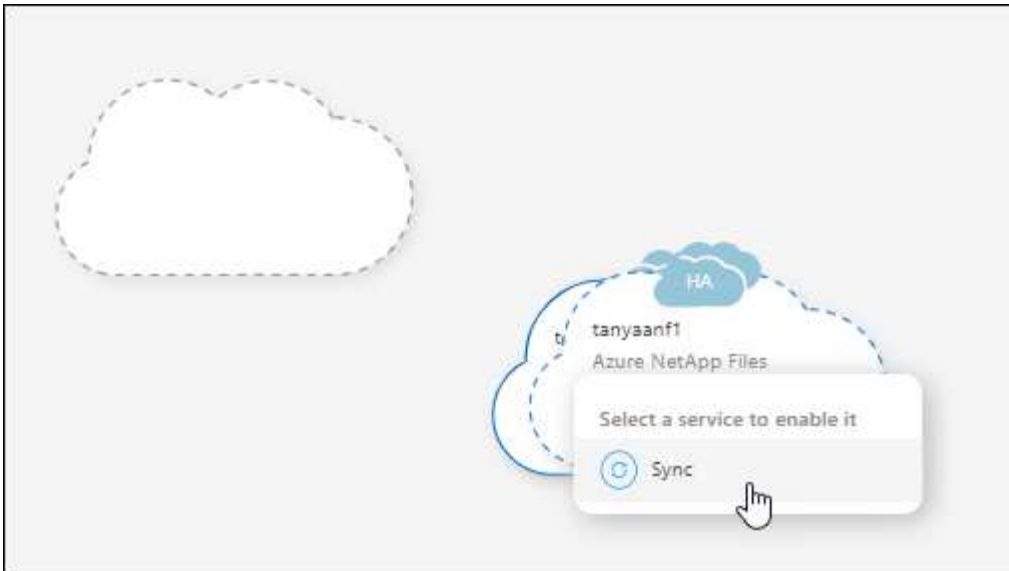
["サポートされている同期関係のリストを表示します"](#)。

同期関係の新しいセットアップ方法が追加されました

BlueXPのCanvasから同期関係を直接設定する方法が追加されました。

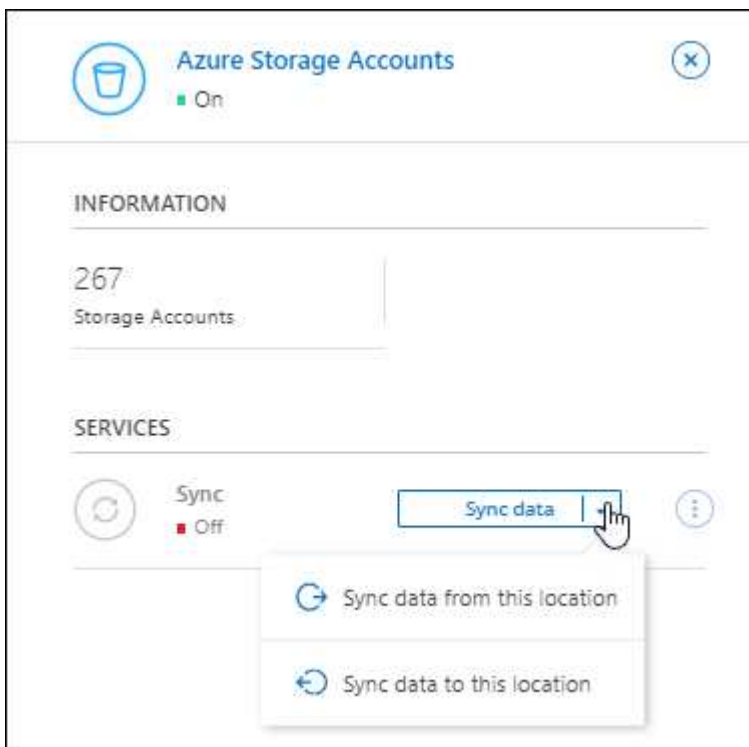
ドラッグアンドドロップ

ある作業環境を別の作業環境の上にドラッグアンドドロップして、キャンバスから同期関係を設定できるようになりました。



右パネル設定

Canvasから作業環境を選択し、右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サーバまたはSMBサーバからAzure Data Lake Storage Gen2へデータを同期できるようになりました。

Azureデータレイク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の接続文字列を指定する必要があります。共有アクセスシグニチャ（SAS）ではなく、通常の接続文字列である必要があります。

す。

"サポートされている同期関係のリストを表示します"。

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、継続的な同期設定がサポートされるようになりました。

Cloud Sync は、初回のデータ同期後、ソースのGoogle Cloud Storageバケットで変更をリスンし、変更が発生した場合は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ストレージ、StorageGRID、またはIBMストレージに同期する場合に使用できます。

データブローカーに関連付けられているサービスアカウントでこの設定を使用するには、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
```

"Continuous Syncの詳細については、こちらをご覧ください"。

新しいGoogle Cloudリージョンサポート

Cloud Sync データブローカーがGoogle Cloudの次の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 (us-east5)
- ダラス (US -サウス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区)

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 -標準-4になりました。

2022年6月6日

継続的な同期

新しい設定を使用すると、ソースのS3バケットからターゲットに変更を継続的に同期できます。

初期データ同期が完了すると、Cloud Sync はソースS3バケットで変更をリスンし、ターゲットへの変更が発生した場合はその変更を継続的に同期します。ソースを定期的に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ストレージ、StorageGRID、またはIBMストレージに同期する場合にのみ使用できます。

データブローカーに関連付けられているIAMロールでは、この設定を使用するために次の権限が必要です。

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

これらの権限は、新しく作成したすべてのデータブローカーに自動的に追加されます。

["Continuous Syncの詳細については、こちらをご覧ください"](#)。

すべての**ONTAP** ボリュームを表示します

同期関係を作成するときに、ソースCloud Volumes ONTAP システム、オンプレミスONTAP クラスタ、またはCloud Sync ONTAP ファイルシステムのFSXにすべてのボリュームが表示されるようになりました。

以前は、Cloud Sync では、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。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に一致しないボリュームや、共有やエクスポートがないボリュームはグレー表示され、選択できません。

Azure Blobへのタグのコピー

Azure Blobがターゲットである同期関係を作成する際に、Cloud Sync でタグをAzure BLOBコンテナにコピーできるようになりました。

- [設定 (* Settings)] ページでは、[*オブジェクトのコピー (* Copy for Objects *)] 設定を使用して、ソースからAzure BLOBコンテナ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機能します。
- * Tags/Metadata* ページで、Azure BLOBコンテナ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、関係のメタデータしか指定できませんでした。

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

2022年5月1日

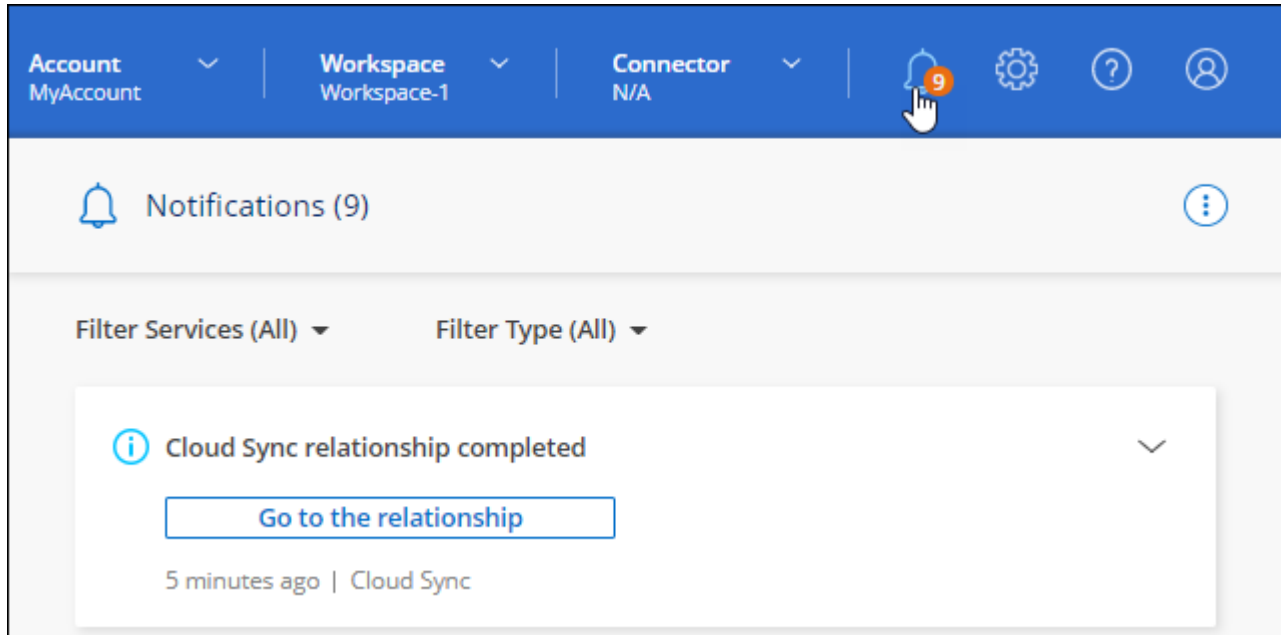
同期タイムアウト

新しい* Sync Timeout *設定を同期関係に使用できるようになりました。この設定を使用すると、指定した時間数または日数内に同期が完了していない場合にCloud Sync でデータの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の詳細については、こちらをご覧ください"](#)。

通知

新しい* Notifications *設定を同期関係に使用できるようになりました。この設定では、BlueXP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。データの同期が成功した場合、データの同期が失敗した場合、データの同期がキャンセルされた場合の通知を有効にできます。



"同期関係の設定の変更の詳細については、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拡張

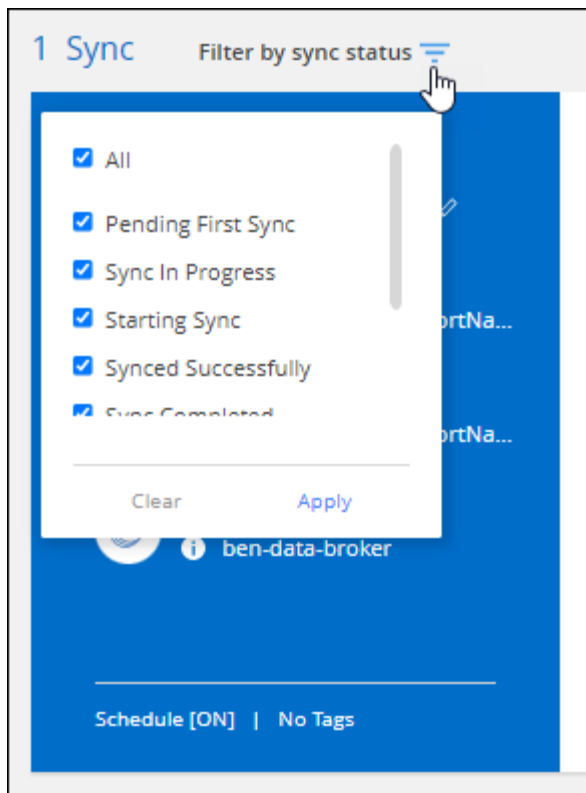
データブローカーグループには、次のような機能拡張が行われました。

- 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設定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について説明します"。

ダッシュボードフィルタ

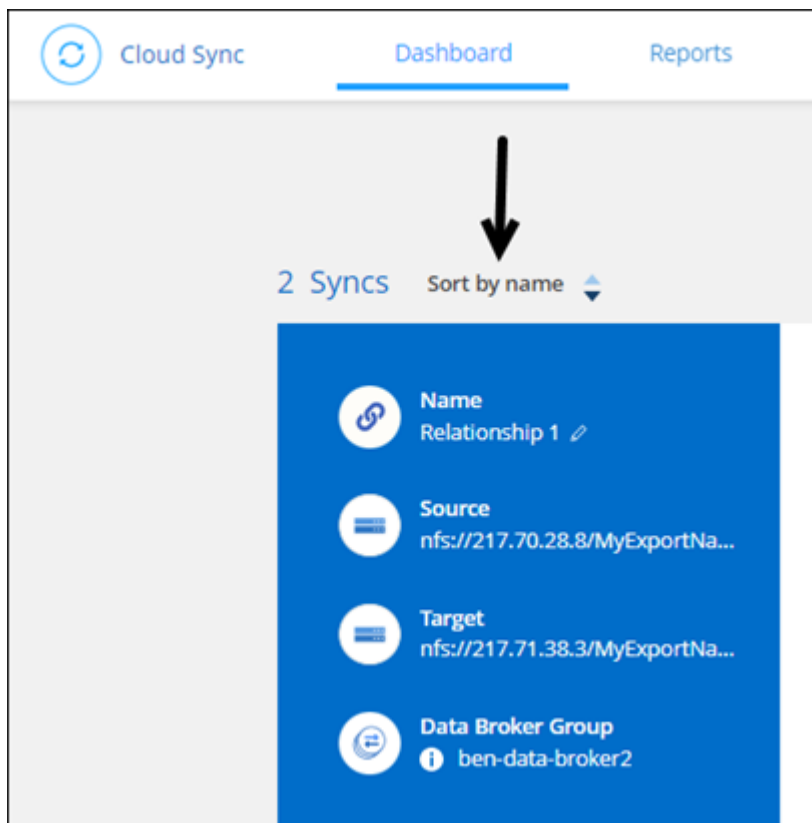
Sync Dashboard の内容をフィルタリングして、特定のステータスに一致する同期関係を簡単に見つけることができるようになりました。たとえば、ステータスが「失敗」の同期関係をフィルタリングできます



2022 年 3 月 3 日

ダッシュボードでソートします

ダッシュボードを同期関係名でソートできるようになりました。



オプションを示すスクリーンショット。"]

データセンスの統合の強化

以前のリリースでは、Cloud Sync とクラウドデータセンスの統合を導入しました。この更新プログラムでは、同期関係を簡単に作成できるように統合を強化しました。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 つの手順で表示されるため、重要な情報をいくつか入力するだけで済みます。

The screenshot shows the 'Selected Data Sense Source' step in the 'Sync Relationship' wizard. The progress bar at the top indicates the current step is 'Data Sense Integration' (1), followed by 'Data Broker Group' (2), 'NFS Server' (3), and 'Directories' (4). A 'How does it work?' link is available. The configuration details for the selected source are as follows:

Source	Host	Working Environment	Volume
Azure NetApp Files	/cifs1	1.1.1.1	cifs

Below the configuration details, a message states: 'A few more things before we continue'. Under the heading 'Define SMB Credentials:', there are three input fields: 'User Name', 'Password', and 'Domain (Optional)'.

2022 年 2 月 6 日

データブローカーグループの機能拡張

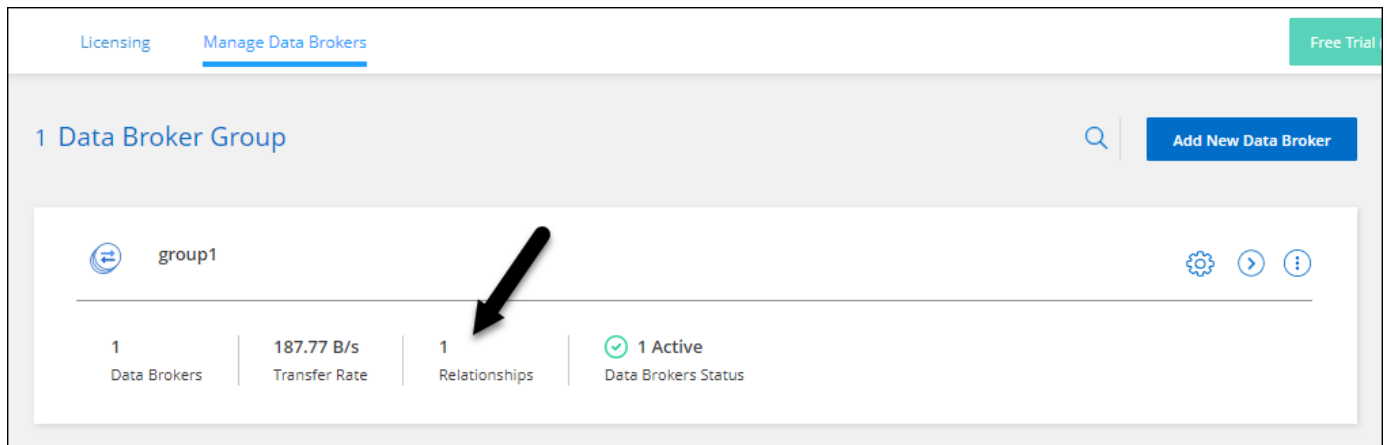
データブローカーの操作方法は、dataBroker_groups_を 強調するように変更されました。

たとえば、新しい同期関係を作成する場合は、特定のデータブローカーではなく、データブローカーの _GROP_To がその関係で使用するように選択します。

The screenshot shows the 'Select a Data Broker Group' step in the 'Sync Relationship' wizard. The progress bar at the top indicates the current step is 'Data Broker Group' (2), preceded by 'SMB Server' (1), followed by 'Shares' (3), and 'Target SMB Server' (4). A 'How does it work?' link is available. The screen displays a list of available data broker groups:

Group Name	Data Brokers	Transfer Rate	Relationships	Data Brokers Status
group1	1	928.43 B/s	0	1 Active

[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できます

レポートの PDF をダウンロードできるようになりました。

"レポートの詳細については、[こちらをご覧ください](#)。"

2022 年 1 月 2 日

新しい **Box** 同期関係

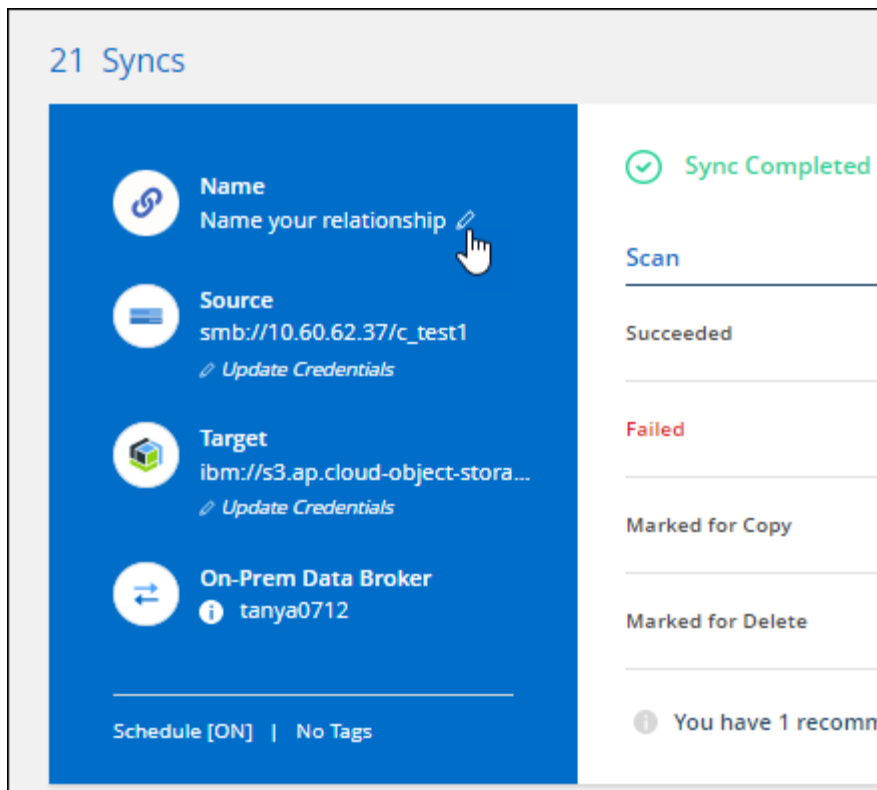
2 つの新しい同期関係がサポートされています。

- Box to Azure NetApp Files の略
- Box から Amazon FSX for ONTAP に移動します

"サポートされている同期関係のリストを表示します"。

関係名

同期関係ごとにわかりやすい名前を指定できるようになり、各関係の目的を簡単に特定できるようになりました。この名前は、関係の作成時および作成後にいつでも追加できます。



S3 プライベートリンク

Amazon S3 との間でデータを同期する際に、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。データブローカーは、ソースからターゲットにデータをコピーする際、プライベートリンクを経由します。

データブローカーに関連付けられている IAM ロールでは、この機能を使用するために次の権限が必要です。

```
"ec2:DescribeVpcEndpoints"
```

この権限は、作成した新しいデータブローカーに自動的に追加されます。

Glacier のインスタント検索

Amazon S3 が同期関係のターゲットである場合に、`_Glacier Instant Retrieve_storage` 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

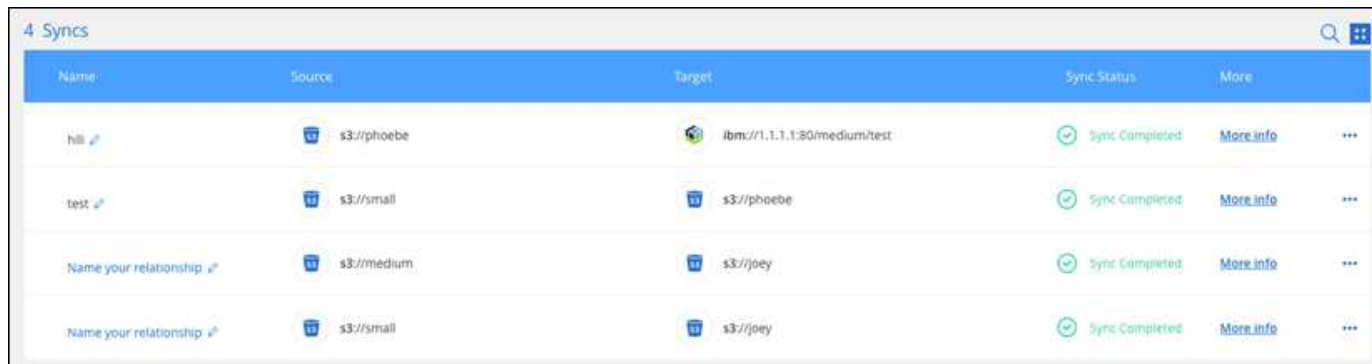
Cloud Sync で、オブジェクトストレージから SMB 共有への ACL のコピーがサポートされるようになりました。これまでは、SMB 共有からオブジェクトストレージへの ACL のコピーのみがサポートされていました。

S3 への SFTP を使用します

SFTP から Amazon S3 への同期関係の作成がユーザ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。

テーブルビューの拡張機能

ダッシュボードのテーブルビューを再設計して使いやすくしました。[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リングして特定の関係に関する詳細情報を表示します。



The screenshot shows a web interface titled "4 Syncs" with a search icon and a grid icon in the top right. Below the title is a table with the following columns: Name, Source, Target, Sync Status, and More. There are four rows of sync relationships, each with a "More info" link and a three-dot menu icon.

Name	Source	Target	Sync Status	More
hll	s3://phoebe	ibmc/71.1.1.1:80/medium/test	Sync Completed	More info
test	s3://small	s3://phoebe	Sync Completed	More info
Name your relationship	s3://medium	s3://joey	Sync Completed	More info
Name your relationship	s3://small	s3://joey	Sync Completed	More info

Jakarta 地域のサポート

Cloud Sync は、AWS アジア太平洋（ジャカルタ）リージョンでのデータブローカーの導入をサポートす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

ソースの 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際に、Cloud Sync で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 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 共有から ACL をコピーする方法について説明します"](#)。

ライセンスを更新します

拡張した Cloud Sync ライセンスを更新できるようになりました。

ネットアップから購入した 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。

["ライセンスを更新する方法について説明します"](#)。

Box の資格情報を更新します

既存の同期関係の Box クレデンシャルを更新できるようになりました。

["クレデンシャルを更新する方法について説明します"](#)。

2021 年 10 月 31 日

ボックスサポート

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

Box は、複数のタイプの同期関係のソースまたはターゲットにすることができます。 ["サポートされている同期関係のリストを表示します"](#)。

作成日の設定

SMB サーバがソースの場合、_Date Created_ という名前の新しい同期関係設定によって、特定の日付以前、特定の日付以前、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 設定の詳細については、こちらをご覧ください"](#)。

2021 年 10 月 4 日

追加のボックスサポート

Cloud Sync で追加の同期関係がサポートされるようになりました ["ボックス"](#) Cloud Sync API を使用する場合：

- Amazon S3 の機能です
- IBM Cloud Object Storage to Box の略
- StorageGRID To Box の略
- Box を NFS サーバに接続します
- Box を SMB サーバーに追加します

["API を使用して同期関係を設定する方法について説明します"](#)。

SFTP パスに関するレポート

次の操作を実行できます。 ["レポートを作成します"](#) SFTP パスの場合

2021 年 9 月 2 日

ONTAP の FSX 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 の詳細をご覧ください"](#)
- ["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について説明します"](#)

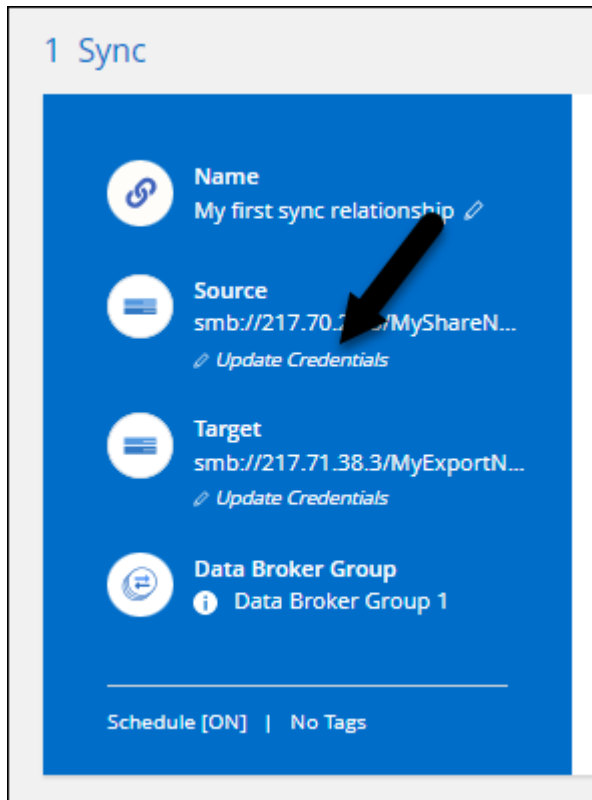
2021 年 8 月 1 日

クレデンシャルを更新

Cloud Sync で、既存の同期関係のソースまたはターゲットの最新のクレデンシャル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。

この拡張機能は、セキュリティポリシーで定期的にクレデンシャルを更新するように要求される場合に役立ちます。 ["クレデンシャルを更新する方法について説明します"](#)。



ページの [資格情報の更新] オプションを示すスクリーンショット。"]

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、同期関係内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、および StorageGRID でサポートされています。

AWS S3 Bucket

Settings

6

Tags/Metadata

7

Review

Relationship Tags

Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket.

This enables you to search for the transferred files by using the tag values.

☒ Save on Object's Tags ☐ Save On Object's Metadata

Tag Key

Up to 128 characters

Tag Value

Up to 256 characters

+

Add Relationship Tag

Optional Field | [Up to 5]

Box のサポート

Cloud Sync は現在サポートされています **"ボックス"** Cloud Sync API を使用する際に、Amazon S3、StorageGRID、IBM Cloud Object Storage との同期関係のソースとして使用。

["API を使用して同期関係を設定する方法について説明します"](#)。

Google Cloud のデータブローカー用パブリック IP

Google Cloud にデータブローカーを導入する際に、仮想マシンインスタンスに対してパブリック 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 にデータブローカーを導入する方法をご確認ください"](#)。

Azure NetApp Files 用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した場合、同期関係用に選択したプロトコルに関係なく、Cloud Sync に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 Storage

Cloud Sync のユーザーインターフェイスで、ONTAP S3 ストレージと Google Cloud Storage バケットの間の同期関係がサポートされ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します"](#)。

オブジェクトメタデータタグ

同期関係を作成して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。

["\[オブジェクトのコピー 設定の詳細については、を参照してください\]"](#)。

橋本事業者のためのサポート

Google Cloud サービスアカウントで認証することで、外部の橋本 Vault からクレデンシャル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。

["データブローカーでの橋 Corp Vault の使用の詳細を確認"](#)。

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際に、ターゲットの 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同期関係ウィザードで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に含まれていました。

2021 年 6 月 7 日

Google Cloud のストレージクラス

同期関係のターゲットが Google Cloud Storage バケットの場合、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 では、次のストレージクラスがサポートされます。

- 標準
- ニアライン
- コールドライン（Coldline）
- Archive サービスの略

2021 年 5 月 2 日

レポート内のエラー

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。

["レポートを作成して表示する方法の詳細については、を参照してください 設定"](#)。

属性を比較します

同期関係ごとに新しい * Compare by * 設定を使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ために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 で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の詳細については、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。Cloud Sync にはBlueXPから直接アクセスできるようになりました。BlueXPでは、同じ機能をすべて利用できます。

BlueXPにログインした後、上部の[同期]タブに切り替えて、以前と同様に関係を表示できます。

さまざまなプロジェクトで **Google Cloud** バケットを使用できます

同期関係を設定する際、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指定している場合は、異なるプロジェクトの Google Cloud バケットから選択できます。

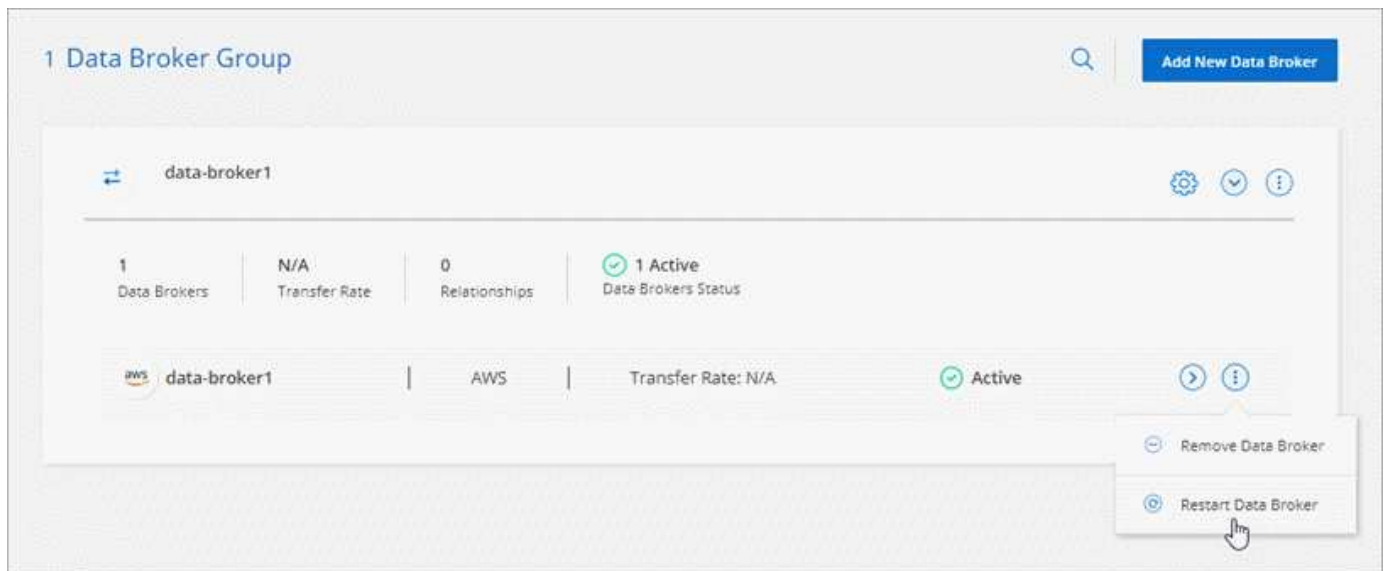
["サービスアカウントの設定方法について説明します"](#)。

Google Cloud Storage と S3 の間のメタデータ

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

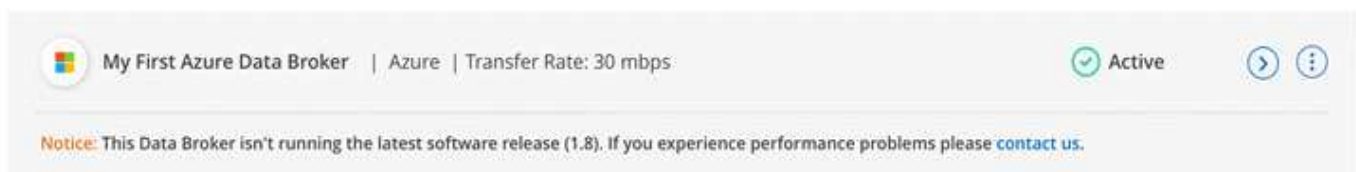
データブローカーを再起動

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に表示されるメッセージです

Cloud Sync は、データブローカーで最新のソフトウェアリリースが実行されていないことを確認できるようになりました。このメッセージは、最新の機能を実際に利用するために役立ちます。



制限

既知の制限事項は、このリリースの製品でサポートされていないプラットフォーム、デバイス、機能、または製品と正しく相互運用できない機能を特定します。これらの制限

事項を慎重に確認してください

BlueXPのコピーと同期は、次の地域ではサポートされません。

- AWSの行政機関向けのサービスです
- Azure Governmentリージョン
- 中国

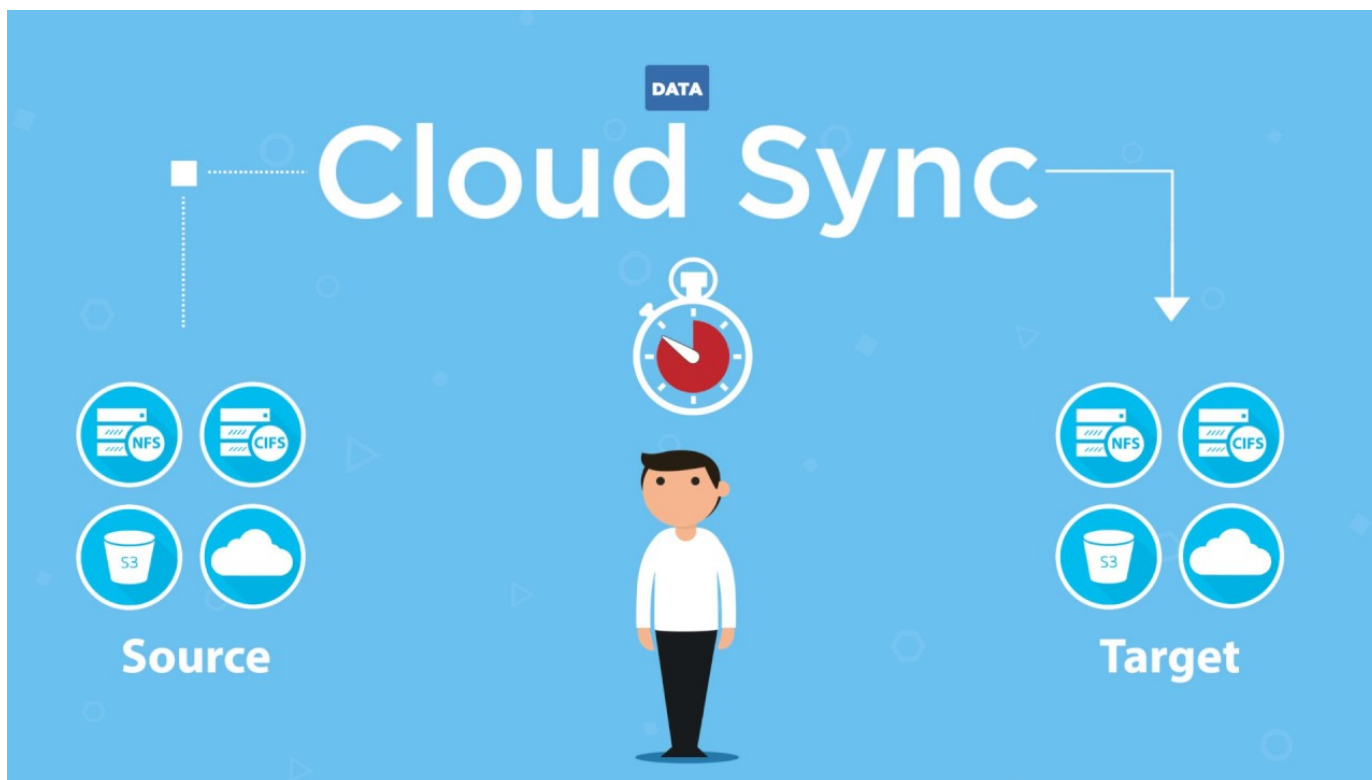
はじめに

BlueXPのコピーと同期の概要

NetApp BlueXPのコピーと同期サービスは、クラウドかオンプレミスかを問わず、シンプルかつセキュアで自動化された方法でデータをあらゆるターゲットに移行します。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、その他のクラウドプロバイダのオブジェクトストアのいずれであっても、BlueXPのコピーと同期を変換して移動できます。

の機能

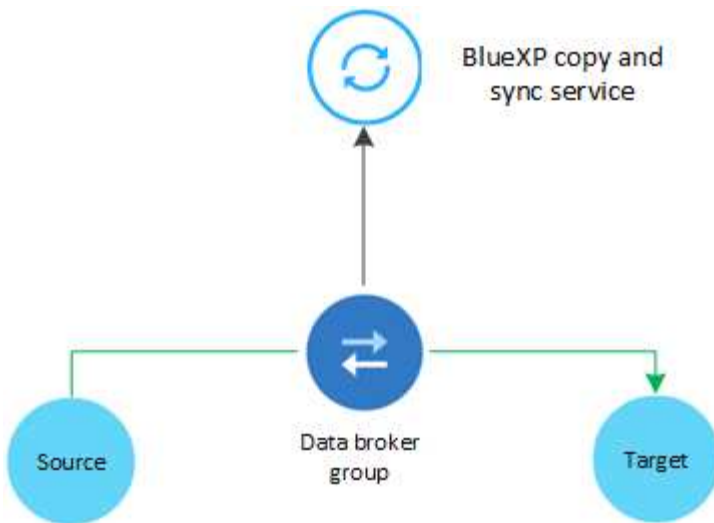
BlueXPのコピーと同期の概要については、次のビデオをご覧ください。



BlueXPのコピーと同期の仕組み

BlueXPのコピーと同期は、データブローカーグループ、BlueXPで利用できるクラウドベースのインターフェイス、ソースとターゲットで構成されるソフトウェアサービス（SaaS）プラットフォームです。

次の図は、BlueXPの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。



ネットアップの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へデータを同期します（これを「`a_sync relationship_`」と呼びます）。データブローカーは、AWS、Azure、Google クラウドプラットフォーム、または社内で行えます。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は、BlueXPのコピーおよび同期サービスと通信し、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経由のアウトバウンド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します。"](#)

最初のコピーの後、設定したスケジュールに基づいて変更されたデータが同期されます。

サポートされているストレージタイプ

BlueXPのコピーと同期では、次のストレージタイプがサポートされます。

- 任意の NFS サーバ
- 任意の SMB サーバ
- Amazon EFS
- ONTAP 対応の Amazon FSX
- Amazon S3
- Azure Blob の略
- Azure Data Lake Storage Gen2
- Azure NetApp Files の特長
- Box （プレビュー版として利用可能）
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google クラウドストレージ
- Googleドライブ
- IBM クラウドオブジェクトストレージ
- オンプレミスの ONTAP クラスタ
- ONTAP S3 ストレージ

- SFTP（APIのみを使用）
- StorageGRID

"サポートされている同期関係を表示します"。

コスト

BlueXPの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

リソースの料金は、1つ以上のデータブローカーをクラウドで実行する場合のコンピューティングとストレージのコストに関連します。

サービス料金

14日間の無料トライアル終了後に、同期関係の料金を支払う方法は2通りあります。1つ目は、AWSまたはAzureから登録する方法です。AWSまたはAzureを利用すると、1時間ごとまたは1年ごとに料金を支払うことができます。2つ目の選択肢は、ネットアップ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ご確認ください"。

BlueXPのコピーと同期のクイックスタート

BlueXPのコピーと同期サービスは、いくつかの手順で開始できます。

1

ログインして**BlueXP**をセットアップします

BlueXPを使い始めました。これにはログイン、アカウントの設定、コネクタの展開、作業環境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、最初に作業環境を作成または検出する必要があります。

- ONTAP 対応の Amazon FSX
- Azure NetApp Files の特長
- Cloud Volumes ONTAP
- オンプレミスの ONTAP クラスタ

Cloud Volumes ONTAP、オンプレミスONTAP クラスタ、およびONTAP 対応Amazon FSXには、コネクタが必要です。

- "BlueXPの使用を開始する方法について説明します"
- "コネクタの詳細については、こちらをご覧ください"

2

ソースとターゲットを準備します

ソースとターゲットがサポートされ、セットアップ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との間の接続を検証することです。

- "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します"

3

ネットアップデータブローカーの設置場所を準備します

ネットアップの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へデータを同期します（これを「a_sync relationship_」と呼びます）。データブローカーは、AWS、Azure、Google クラウドプラットフォーム、または社内で行うことができます。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は、BlueXPのコピーおよび同期サービスと通信し、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経由のアウトバウンド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します。](#)"。

BlueXPのコピーと同期は、ガイドに従ってインストールプロセスを実行して同期関係を作成します。同期関係を作成したら、データブローカーをクラウドに導入したり、自社の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します](#)"
- "[Azure のインストールを確認します](#)"
- "[Google Cloud のインストール状況を確認します](#)"
- "[Linux ホストのインストールを確認します](#)"

4

最初の同期関係を作成します

にログインします "[BlueXP](#)"をクリックし、*[同期]*を選択し、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。プロンプトに従ってセットアップを完了します。 "[詳細はこちら。](#)"。

5

無料トライアルが終了したら、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の支払いを申し込むことができます。または、ネットアップから直接ライセンスを購入することもできます。BlueXPのコピーの[License Settings]ページに移動して同期するだけでセットアップできます。 "[詳細はこちら。](#)"。

サポートされている同期関係

BlueXPのコピーと同期を使用すると、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。サポートされている関係を理解してから開始する必要があります。

ソースの場所	サポートされるターゲットロケーション
Amazon EFS	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID
ONTAP 対応の Amazon FSX	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
Amazon S3	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • ボックス ^1 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure Blob の略	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
Azure Data Lake Storage Gen2	<ul style="list-style-type: none"> • Azure NetApp Files の特長 • Cloud Volumes ONTAP • FSX for ONTAP の略 • IBM クラウドオブジェクトストレージ • NFS サーバ • On-Prem ONTAP の略 • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure NetApp Files の特長	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID
ボックス ^1	<ul style="list-style-type: none"> • ONTAP 対応の Amazon FSX • Amazon S3 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • IBM クラウドオブジェクトストレージ • NFS サーバ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID
Cloud Volumes Service	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
Google クラウドストレージ	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Googleドライブ	<ul style="list-style-type: none"> • NFS サーバ • SMB サーバ
IBM クラウドオブジェクトストレージ	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • ボックス ^1 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
NFS サーバ	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • Googleドライブ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
オンプレミスの ONTAP クラスタ	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
ONTAP S3 ストレージ	<ul style="list-style-type: none"> • Amazon S3 • Azure Data Lake Storage Gen2 • Google クラウドストレージ • NFS サーバ • SMB サーバ • StorageGRID • ONTAP S3 ストレージ
SFTP ²	S3
SMB サーバ	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • Googleドライブ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
StorageGRID	<ul style="list-style-type: none"> • Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • ボックス ^1 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • 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、BlueXPのコピーおよび同期APIでのみサポートされます。
3. BLOB コンテナがターゲットの場合は、特定の Azure BLOB ストレージ階層を選択できます。
 - ホットストレージ
 - 優れたストレージ
4. [[storage-classes]] 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（これがデフォルトクラス）
 - インテリジェント階層化
 - 標準的なアクセス頻度は低い
 - 1 回のアクセスではほとんど発生しません
 - Glacier Deep Archive
 - Glacierの柔軟な取得
 - Glacier のインスタント検索
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。
 - 標準

- ニアライン
- コールドライン（Coldline）
- Archive サービスの略

ソースとターゲットを準備します

ソースとターゲットが次の要件を満たしていることを確認します。

ネットワーキング

- ソースとターゲットに、データブローカーグループへのネットワーク接続が必要です。

たとえば、NFS サーバ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、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。

- 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ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

ターゲットディレクトリ

同期関係を作成する際、BlueXPのコピーと同期を使用して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を作成できます。そのため、優先ターゲットディレクトリがすでに存在していることを確認してください。

ディレクトリを読み取るための権限

BlueXPのコピーと同期には、ソースまたはターゲット内のすべてのディレクトリやフォルダを表示するための読み取り権限が必要です。

NFS

ファイルおよびディレクトリに対して、ソース / ターゲットに uid / gid を指定して権限を定義しておく必要があります。

オブジェクトストレージ

- AWS と Google Cloud の場合、データブローカーにはリストオブジェクトの権限が必要です（データブローカーのインストール手順を実行する場合、これらの権限はデフォルトで提供されます）。
- Azure 、 StorageGRID 、 IBM の場合は、同期関係のセットアップ時に入力するクレデンシャルに、リストオブジェクトの権限が必要です。

SMB

同期関係のセットアップ時に入力する SMB クレデンシャルには、リストフォルダの権限が必要です。



データブローカーでは、デフォルトで、.snapshot、~snapshot、.copy-Offload の各ディレクトリが無視されます

[s3] 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ます。

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では、AWS または社内にデータブローカーを導入する必要があります。いずれの場合も、BlueXPのコピーと同期で、インストール時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について説明します"](#)
- ["Linux ホスト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"](#)

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

同期関係をセットアップする際、データブローカーに関連付けられていない AWS アカウントに配置されている S3 バケットを指定することができます。

["この JSON ファイルに含まれている権限"](#) データブローカーがアクセスできるように、S3 バケットに適用する必要があります。これらの権限を使用すると、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、バケット内のオブジェクトを一覧表示できます。

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。
 - データブローカーを Linux ホストに手動でインストールした場合、データブローカーの導入時に AWS クレデンシャルを指定した AWS ユーザの ARN を `_RoleARN_` should be the ARN when deploying a AWS credentials
 - CloudFormation テンプレートを使用して AWS にデータブローカーを導入した場合は、テンプレートによって作成された IAM ロールの ARN を `_RoleARN_` にする必要があります。

ロールARNを確認するには、EC2コンソールに移動してデータブローカーインスタンスを選択し、概要タブからIAMロールを選択します。次に、ロール ARN を含む IAM コンソールに概要ページが表示されます。

Summary

Delete role

Role ARN `arn:aws:iam::142991742681:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

Role description [Edit](#)

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ます。

Azure BLOB でサポートされるデータブローカーの場所

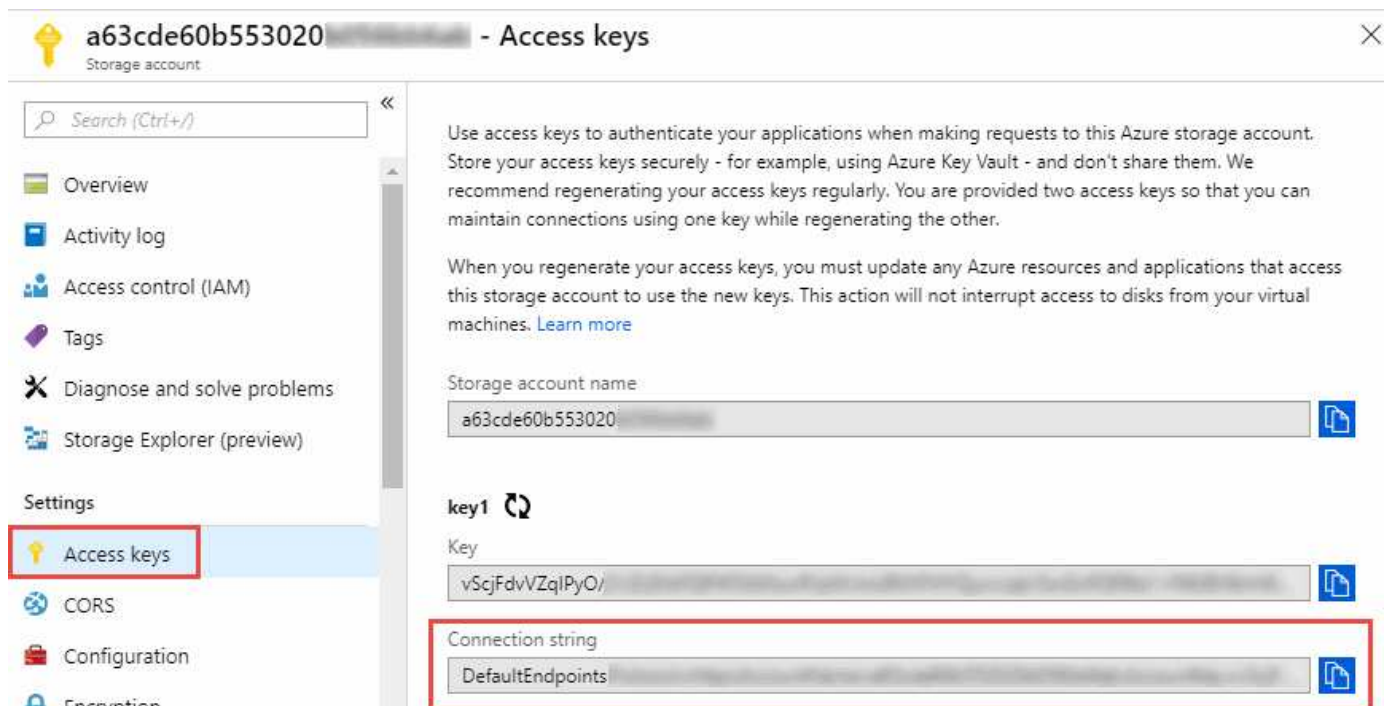
データブローカーは、同期関係に Azure BLOB ストレージが含まれている場合でも、任意の場所に配置できます。

サポートされている Azure リージョン

中国、米国政府、米国国防総省を除くすべての地域がサポートされます。

Azure Blob および NFS / SMB を含む関係の接続文字列

Azure Blob コンテナと NFS または SMB サーバの間の同期関係を作成する場合は、BlueXP のコピーとストレージアカウント接続文字列との同期を指定する必要があります。



The screenshot shows the 'Access keys' page for an Azure storage account. The left sidebar has 'Access keys' selected. The main content area includes instructions on using access keys, the storage account name 'a63cde60b553020', and two keys. The 'key1' section shows a key and a connection string 'DefaultEndpoints' which is highlighted with a red box.

を選択すると表示されます。"]

2 つの Azure Blob コンテナ間でデータを同期する場合は、接続文字列にを含める必要があります **"共有アクセスシグニチャ"**（SAS）。BLOB コンテナと NFS サーバまたは SMB サーバの間で同期する場合は、SAS を使用することもできます。

SA は、BLOB サービスとすべてのリソースタイプ（サービス、コンテナ、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： read および list
- ターゲット BLOB コンテナの場合：読み取り、書き込み、一覧表示、追加、作成

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Storage Explorer (preview)
- Settings
 - Access keys
 - CORS
 - Configuration
 - Encryption
 - Shared access signature**
 - Firewalls and virtual networks
 - Advanced Threat Protection (pr...
 - Properties
 - Locks

Allowed services ⓘ

☒ Blob
☐ File
☐ Queue
☐ Table

Allowed resource types ⓘ

☒ Service
☒ Container
☒ Object

Allowed permissions ⓘ

☒ Read
☒ Write
☒ Delete
☒ List
☒ Add
☒ Create
☐ Update
☐ Process

Start and expiry date/time ⓘ

Start

End

Allowed IP addresses ⓘ

Allowed protocols ⓘ

☒ HTTPS only
☐ HTTPS and HTTP

Signing key ⓘ

Generate SAS and connection string

を選択すると表示されます。"]

Azure BLOBコンテナを含むContinuous Sync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接続文字列を使用している場合は、近い将来有効期限が切れるように設定しないでください。

Azure Data Lake Storage Gen2

Azure Data Lakeを含む同期関係を作成する場合は、BlueXPのコピーとストレージアカウントの接続文字列との同期を指定する必要があります。共有アクセスシグニチャ（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。ディスクのサービスレベルが Standard の場合は、エラーやパフォーマンスの問題が発生することがあります。

適切なサービスレベルの決定に支援が必要な場合は、ソリューションアーキテクトに相談してください。取得できるスループットはボリュームサイズとボリューム階層によって決まります。

39

"Azure NetApp Files のサービスレベルとスループットの詳細については、[こちらをご覧ください](#)。"

Box の要件

- Box を含む同期関係を作成するには、次の資格情報を入力する必要があります。
 - クライアント ID
 - クライアントシークレット
 - 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、統合構成のデータブローカーグループを使用し、次の設定を 1 にする必要があります。
 - スキャナの同時実行数
 - スキャナ処理の上限
 - 転送元同時実行数
 - 転送元プロセスの制限

["データブローカーグループのユニファイド構成を定義する方法について説明します"](#)。

Google Cloud Storageバケットの要件

Google クラウドストレージバケットが次の要件を満たしていることを確認します。

Google クラウドストレージでサポートされるデータブローカーの場所

Google Cloud Storage を含む同期関係を確立するには、Google Cloud または自社運用環境にデータブローカーを導入する必要があります。BlueXPのコピーと同期を使用すると、データブローカーのインストールプロセスに従って同期関係を作成できます。

- ["Google Cloud データブローカーの導入方法をご確認ください"](#)
- ["Linux ホスト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"](#)

サポートされている Google Cloud リージョン

すべてのリージョン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際、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指定している場合は、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について説明します"](#)。

SnapMirror デスティネーションの権限

同期関係のソースが SnapMirror デスティネーション（読み取り専用）の場合、「読み取り / リスト」権限でソースからターゲットにデータを同期できます。

Google Cloudバケットの暗号化

お客様が管理するKMSキーまたはGoogleが管理するデフォルトのキーを使用して、ターゲットのGoogle Cloudバケットを暗号化できます。バケットにKMS暗号化がすでに追加されている場合は、Googleが管理するデフォルトの暗号化よりも優先されます。

お客様が管理するKMSキーを追加するには、**"正しい権限"**、および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、次の情報を入力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電子メールアドレス
- Google Driveへのアクセス権限を持つGoogle CloudサービスアカウントのEメールアドレスです
- 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のドキュメントに記載されている手順に従います。

- **"サービスアカウントとクレデンシャルを作成します"**
- **"ドメイン全体の権限をサービスアカウントに委任します"**

OAuth Scopesフィールドを編集する場合は、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 サーバには、NetApp システムまたは NetApp 以外のシステムを使用できます。
- ファイルサーバは、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。

サーバで目的のバージョンが有効になっている必要があります。

- 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_starting` です。

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。これは ACL をコピーするために必要です。

ONTAP S3 ストレージの要件

を含む同期関係を設定する場合 **"ONTAP S3 ストレージ"**を使用するには、次のものを用意する必要があります。

- ONTAP に接続されている LIF の IP アドレス S3
- ONTAP が設定されているアクセスキーとシークレットキー を使用してください

SMB サーバの要件

- SMB サーバは、NetApp システムまたは他社製システムのいずれかです。
- BlueXPのコピーと同期を、SMBサーバに対する権限があるクレデンシャルで指定する必要があります。
 - ソース SMB サーバについては、list および read という権限が必要です。

Backup Operators グループのメンバーは、ソース SMB サーバでサポートされています。

- ターゲット SMB サーバについては、list、read、および write の各権限が必要です。
- ファイルサーバは、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、および 3.11 がサポートされます。
- 「フルコントロール」権限を持つ「管理者」グループにソースフォルダとターゲットフォルダを付与します。

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。この場合、"getxattr error 95" というエラーが表示されます。

非表示のディレクトリとファイルに関する SMB の制限

SMB の制限は、SMB サーバ間でデータを同期する際に非表示のディレクトリとファイルに影響します。ソース SMB サーバ上のディレクトリまたはファイルが Windows で非表示になっていた場合、非表示属性はターゲット SMB サーバにコピーされません。

大文字と小文字の区別がないため、**SMB** 同期の動作が制限されます

SMB プロトコルでは大文字と小文字が区別されないため、大文字と小文字は同じものとして扱われます。この動作により、ターゲットに SMB サーバとデータがすでに存在する同期関係では、ファイルが上書きされ、ディレクトリのコピーで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て、BlueXPのコピーと同期で「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」がソースのファイル「A」で上書きされます。

ディレクトリの場合は、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て、BlueXPのコピーと同期で「b」というディレクトリをターゲットにコピーしようすると、ディレクトリがすでに存在することを示すエラーがBlueXPのコピーと同期に表示されます。そのため、BlueXPのコピーと同期で「B」というディレクトリのコピーが常に失敗します。

この制限を回避する最善の方法は、空のディレクトリにデータを確実に同期させることです。

BlueXPのコピーと同期のネットワークの概要

BlueXPのコピーと同期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とターゲットの場所の間の接続、データブローカーからのポート443経由のアウトバウンド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

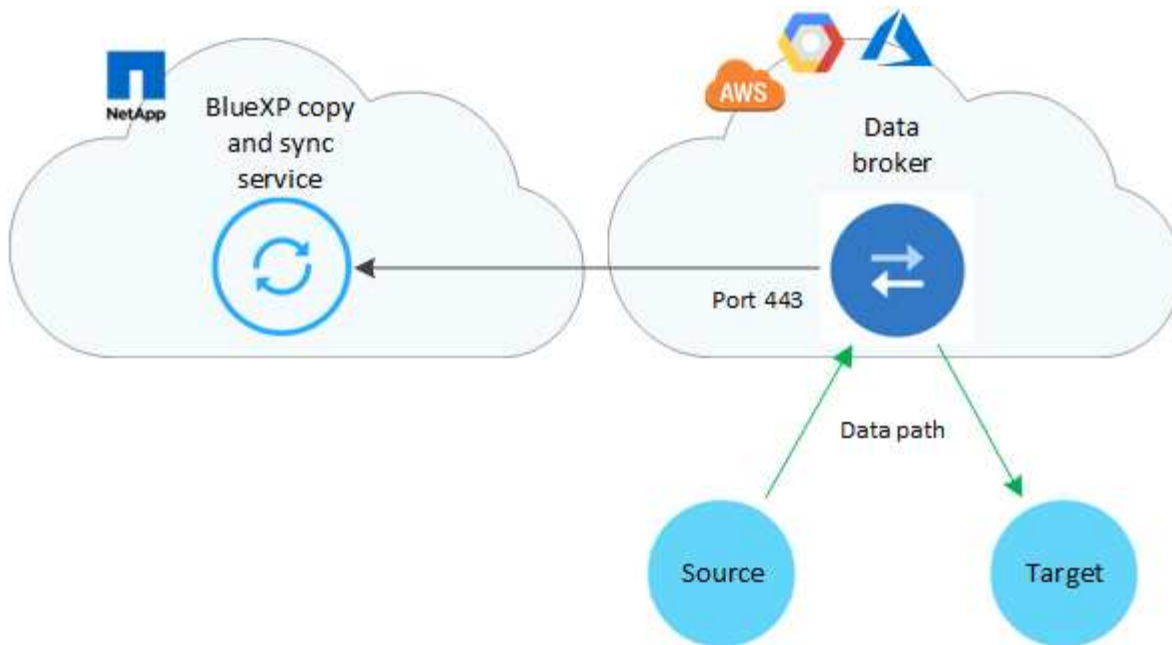
データブローカーグループは、クラウドまたはオンプレミスにインストールされた 1 つ以上のデータブローカーで構成されます。

クラウド内のデータブローカー

次の図は、クラウド、AWS、Google Cloud、Azure で実行されるデータブローカーを示しています。データブローカーへの接続が確立されていれば、ソースとターゲットはどの場所にも存在できます。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 接続があるとして。

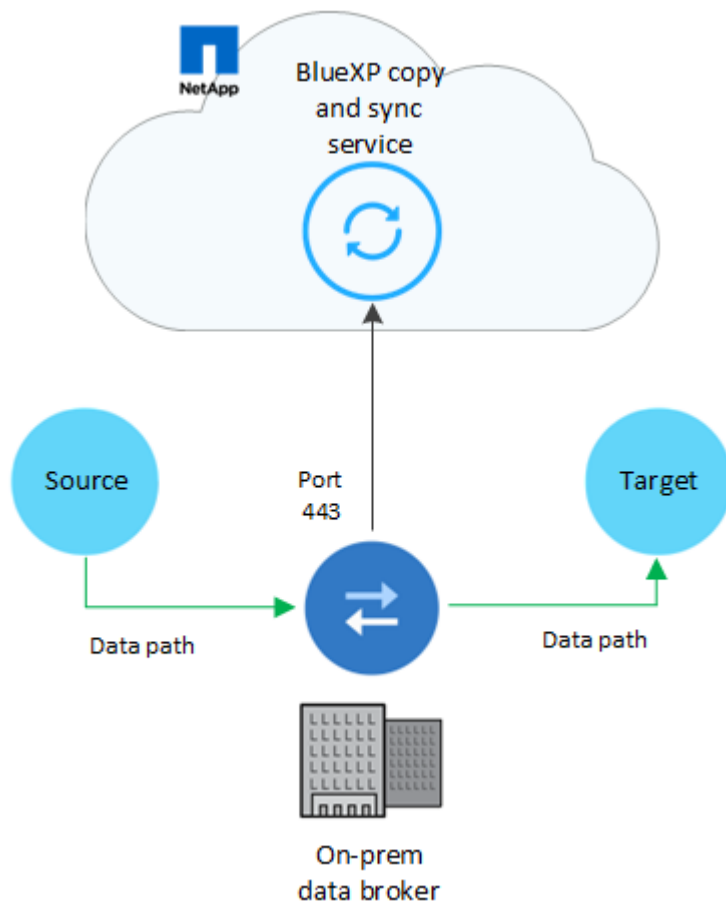


BlueXPのコピーと同期でデータブローカーをAWS、Azure、Google Cloudに導入すると、必要なアウトバウンド通信を可能にするセキュリティグループが作成されます。



社内のデータブローカー

次の図は、データセンターで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。この場合も、データブローカーに接続が確立されていれば、ソースとターゲットはどの場所にも存在できます。



ネットワーク要件

- ・ソースとターゲットに、データブローカーグループへのネットワーク接続が必要です。

たとえば、NFS サーバ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、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。

- ・データブローカーがBlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるようにするには、アウトバウンドインターネット接続が必要です。
- ・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ソース、ターゲット、データブローカーを設定することを推奨します。3つのコンポーネント間の時間差は5分を超えないようにしてください。

ネットワークエンドポイント

ネットアップのデータブローカーがBlueXPのコピーおよび同期サービスと通信し、他のいくつかのサービスやリポジトリにアクセスするには、ポート443経由のアウトバウンドインターネットアクセスが必要です。ローカル Web ブラウザでは、特定の操作を実行するためにエンドポイントへのアクセスも必要です。発信接続を制限する必要がある場合は、発信トラフィック用にファイアウォールを設定する際に、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アクセスします。

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に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 :	node.js、NPM、および開発に使用されているその他のサードパーティパッケージを更新するためのリポジトリに問い合わせます。
\ https://tgz.pm2.io	では、PM2を更新するためのリポジトリにアクセスします。PM2は、BlueXPのコピーと同期の監視に使用するサードパーティパッケージです。
¥ https://sqs.us-east-1.amazonaws.com ¥ https://kinesis.us-east-1.amazonaws.com	BlueXPのコピーと同期が処理（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のサービスにアクセスするため。
¥ https://s3.region.amazonaws.com （例： s3.us-east-2.amazonaws.com:443 ） https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region ["S3 エンドポイントの一覧については、AWS の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 に連絡する。
\ https://s3.amazonaws.com/	BlueXPのコピーと同期からデータブローカーの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圧縮し、us-east-1リージョン内の事前定義されたS3バケットにログをアップロードします。

エンドポイント	目的
\ https://storage.googleapis.com/	同期関係でGCPバケットを使用している場合にGoogle Cloudに連絡するには、次の手順に従います。
https://storage-account.blob.core.windows.netAzure Data Lake Gen2を使用する場合 ： https://storage-account.dfs.core.windows.net[]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	BlueXPのコピーと同期サービスにお問い合わせください。
\ https://support.netapp.com	同期関係に BYOL ライセンスを使用する場合は、ネットアップの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 をインストールするには、AutoSupport メッセージをネットアップテクニカルサポートに送信するには 7z が必要です。
https://sts.amazonaws.com https://sts.us-east-1.amazonaws.com	データブローカーがAWSに導入されたときや、オンプレミスに導入されてAWSのクレデンシャルが指定されたときに、AWSのクレデンシャルを確認することができます。データブローカーは、導入時、更新時、および再起動時にこのエンドポイントにアクセスします。
¥ https://console.bluexp.netapp.com/ ¥ https://netapp-cloud-account.auth0.com	新しい同期関係のソースファイルを分類を使用して選択する場合には、BlueXPの分類に連絡します。
\ 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.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 ブラウザエンドポイント

トラブルシューティングの目的でログをダウンロードするには、Web ブラウザから次のエンドポイントにアクセスする必要があります。

データブローカーをインストール

AWS に新しいデータブローカーを作成

新しいデータブローカーグループを作成する場合、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導入します。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

また、クラウド内または社内の既存の 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。["詳細はこちら。"](#)。

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。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

ネットワーク要件

- データブローカーは、BlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるように、アウトバウンドインターネット接続を必要とします。

BlueXPのコピーと同期でAWSにデータブローカーを導入すると、必要なアウトバウンド通信を可能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設定できます。

アウトバウンド接続を制限する必要がある場合は、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- 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、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3つのコンポーネント間の時間差は5分を超えないようにしてください。

AWS にデータブローカーを展開するために必要な権限

の導入に使用する AWS ユーザーアカウント データブローカーの権限は、に含まれている必要があります ["ネットアップが提供するポリシーです"](#)。

[IAM] AWSデータブローカーで独自のIAMロールを使用する必要があります

BlueXPのコピーと同期でデータブローカーを導入すると、データブローカーインスタンス用の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展開できます。組織に厳密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できます。

IAM ロールは、次の要件を満たす必要があります。

- EC2 サービスは、IAM の役割を信頼できるエンティティとして引き受けることを許可されている必要があります。
- "この JSON ファイルで定義されている権限" データブローカーが正しく機能するように、IAM ロールに関連付ける必要があります。

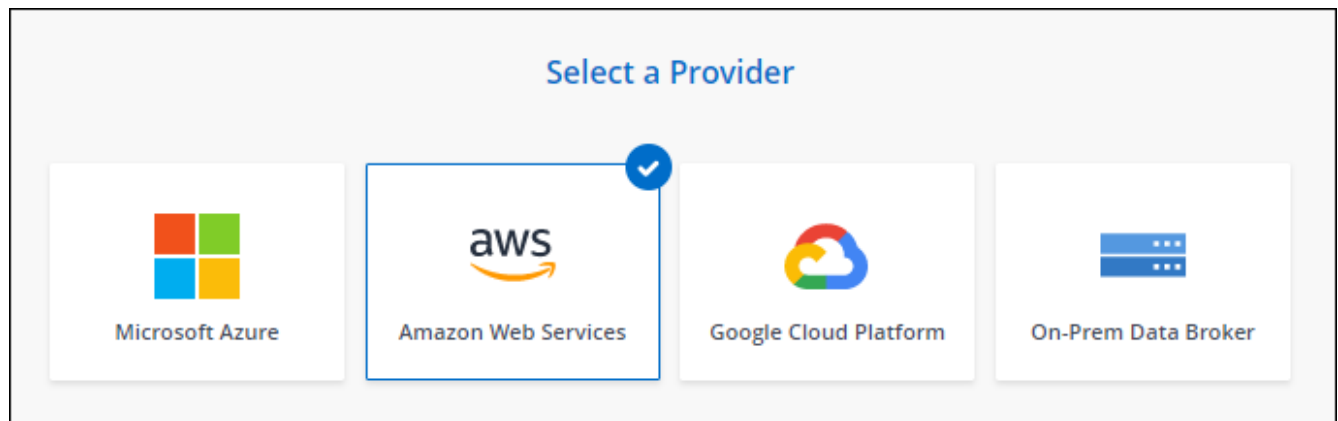
データブローカーを導入する際に IAM ロールを指定するには、次の手順に従います。

データブローカーの作成

新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを AWS にインストールする方法について説明します。

手順

1. [新しい同期の作成]*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、*[続行]*を選択します。
「* データブローカーグループ *」 ページが表示されるまで、手順を完了します。
3. [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。



4. データブローカーの名前を入力し、*[続行]*を選択します。
5. AWSアクセスキーを入力して、BlueXPのコピーと同期がお客様に代わってAWSでデータブローカーを作成できるようにします。

キーは保存されず、他の目的に使用されることもありません。

アクセスキーを提供しない場合は、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、クレデンシャルを指定する必要はありません。

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紹介したビデオを次に示します。

▶ https://docs.netapp.com/ja-jp/bluexp-copy-sync//media/video_cloud_sync.mp4 (video)

6. 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て既存のIAMロールを選択します。または、このフィールドを空白

のままにしてBlueXPのコピーと同期でロールが作成されます。また、KMSキーを使用してデータブローカーを暗号化することもできます。

独自の IAM ロールを選択した場合は、[必要な権限を指定する必要があります](#)。

7. 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、プロキシの設定を指定します。
8. データブローカーが利用可能になったら、BlueXPのコピーと同期で*[続行]*を選択します。

次の図は、AWS に正常に導入されたインスタンスを示しています。

Data Brokers	Transfer Rate	Relationships	Data Brokers Status
1	N/A	0	1 Active

9. ウィザードのページに入力して、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導入し、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は、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

BlueXPのコピーと同期では、次の構成を使用してAWSにデータブローカーが作成されます。

Node.jsとの互換性

v21.2.0

インスタンスタイプ

m5n.xlarge（リージョン内で使用可能な場合）。 m5.xlarge（ 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タイプ

10GB gp2 SSD です

Azure に新しいデータブローカーを作成

新しいデータブローカーグループを作成する場合は、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導入します。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

また、クラウド内または社内の既存の 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。["詳細はこちら。"](#)。

サポートされている Azure リージョン

中国、米国政府、米国国防総省を除くすべての地域がサポートされます。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

ネットワーク要件

- データブローカーは、BlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるように、アウトバウンドインターネット接続を必要とします。

BlueXPのコピーと同期でAzureにデータブローカーを導入すると、必要なアウトバウンド通信を可能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、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- 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、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3つのコンポーネント間の時間差は5分を超えないようにしてください。

Azureにデータブローカーを導入するための権限が必要です

データブローカーの導入に使用するAzureユーザアカウントに、次の権限があることを確認してください。

```
{
  "Name": "Azure Data Broker",
  "Actions": [
    "Microsoft.Resources/subscriptions/read",
    "Microsoft.Resources/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Compute/disks/write",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/virtualNetworks/read",
```

```

        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/publicIPAddresses/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Storage/storageAccounts/read",

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

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

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

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

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

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

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

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

```

```

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

```

注：

1. 次の権限は、"[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で次の手順を実行します。

- 'microsoft.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.StorageAccounts/write'

また、AzureにContinuous Syncを実装する場合は、割り当て可能な範囲をサブスクリプションの範囲に設定し、*リソースグループの範囲ではない*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/networkSecurityGroups/securityRules/read"
- Microsoft.Network/networkSecurityGroups/read"

認証方式

データブローカーを導入する場合、仮想マシンの認証方式として、パスワードまたはSSH公開鍵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、を参照してください "[Azure のドキュメント：「Create and use an SSH public-private key pair for Linux VMs in Azure」](#)"。

データブローカーの作成

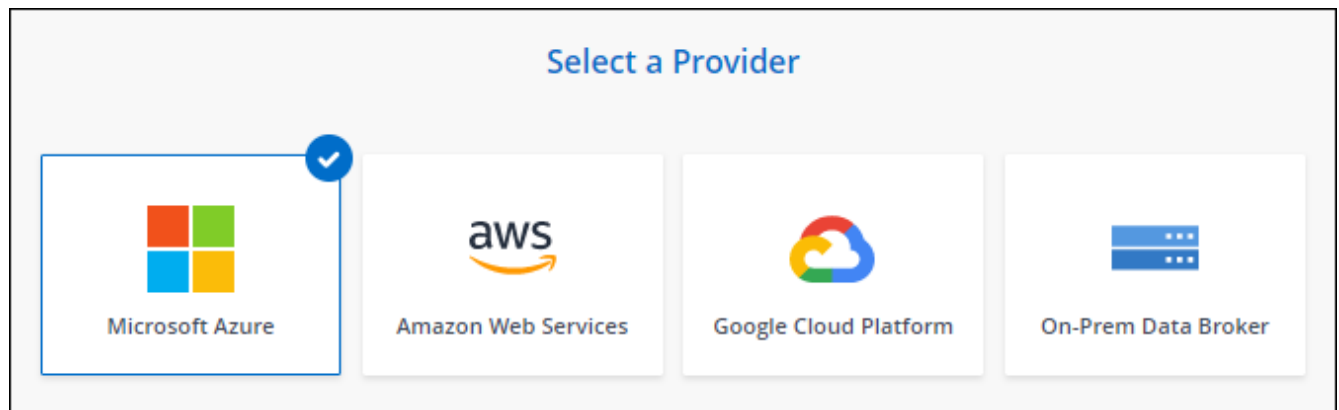
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを Azure にインストールする方法について説明します。

手順

1. [新しい同期の作成]*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、*[続行]*を選択します。

「* データブローカーグループ *」 ページが表示されるまで、手順を完了します。

3. [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。



4. データブローカーの名前を入力し、*[続行]*を選択します。
5. 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 が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

6. 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。



Continuous Sync関係を実装する場合は、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。

7. 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、プロキシ設定を指定します。
8. 「 * Continue * 」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のアクセスキーとシークレットキーを入力します。
9. [続行]*を選択し、展開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 分かかることがあります。

10. BlueXPのコピーと同期で、データブローカーが利用可能になったら*[続行]*を選択します。
11. ウィザードのページに入力して、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導入し、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、追加の同期関係とともに使用できます。

管理者の同意が必要なことを示すメッセージを受信しますか？

BlueXPのコピーと同期には組織内のリソースにユーザに代わって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ことをMicrosoftから通知された場合は、次の2つの方法があります。

1. AD 管理者に次の権限を提供するよう依頼します。

Azure では、[管理センター] > [Azure AD] > [ユーザーとグループ] > [ユーザー設定 *] の順に選択し、* ユーザーが代わりに会社のデータにアクセスするアプリに同意できるようにします。 *

2. 次の URL を使用して、* CloudSync-AzureDataBrokerCreator* に代わって、AD 管理者に同意するよう依頼してください（これは管理者同意エンドポイントです）。

\ https://login.microsoftonline.com/{FILL テナント ID }/v2.0/adminconsent?client_id=8ee4ca3a-BAFA-4831-97cc-5a38923cab85 &redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read に移動します

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

データブローカー VM の詳細

BlueXPのコピーと同期では、Azureで次の構成を使用してデータブローカーが作成されます。

Node.jsとの互換性

v21.2.0

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

Rocky Linux 9.0

ディスクのサイズとタイプ

64 GB Premium SSD

Google Cloud で新しいデータブローカーを作成

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導入します。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

また、クラウド内または社内の既存の 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。["詳細はこちら。"](#)

サポートされている **Google Cloud** リージョン

すべてのリージョンがサポートされています。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

ネットワーク要件

- データブローカーは、BlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるように、アウトバウンドインターネット接続を必要とします。

BlueXPのコピーと同期でGoogle Cloudにデータブローカーを導入すると、必要なアウトバウンド通信を可能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、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- 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、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3つのコンポーネント間の時間差は5分を超えないようにしてください。

Google Cloud にデータブローカーを導入するための権限が必要です

データブローカーを導入する 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導入する場合、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」権限が必要なのは、外部の橋本ボルトを使用するようにデータブローカーを設定する予定の場合のみです。
2. 「pubsub.*」権限と「storage.enable」は、Google Cloud Storageから別のクラウドストレージ上の同期関係に対してContinuous Sync設定を有効にする場合にのみ必要です。 ["継続的同期オプションの詳細については、こちらをご覧ください"](#)。
3. 「cloudkms.cryptoKeys.list」権限と「cloudkms.keyrings.list」権限は、ターゲットのGoogle Cloud

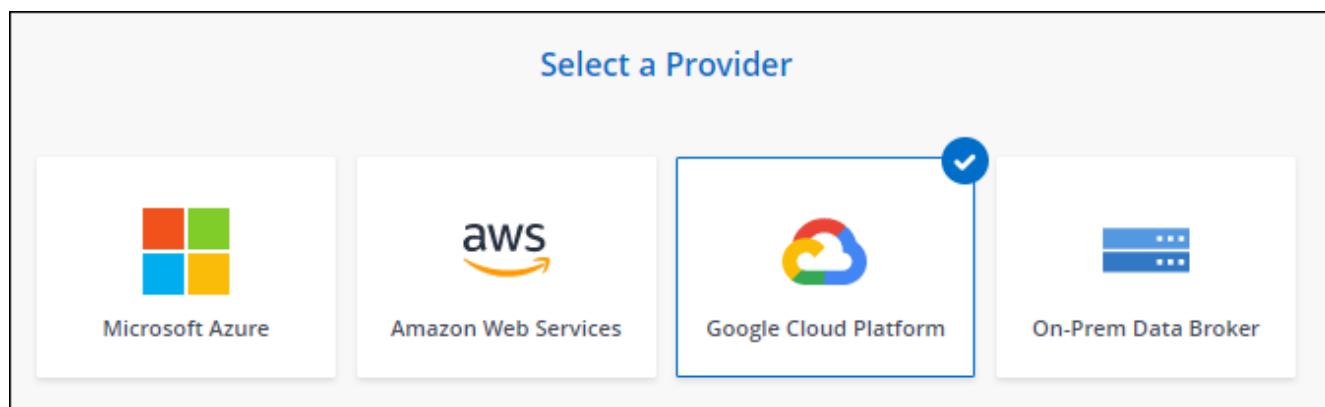
Storageバケットで顧客管理KMSキーを使用する場合にのみ必要です。

データブローカーの作成

新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成するときにデータブローカーを Google Cloud にインストールする方法について説明します。

手順

1. [新しい同期の作成]*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、*[続行]*を選択します。
「* データブローカーグループ*」ページが表示されるまで、手順を完了します。
3. [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。



4. データブローカーの名前を入力し、*[続行]*を選択します。
5. メッセージが表示されたら、Google アカウントでログインします。

このフォームは Google が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

6. プロジェクトとサービスアカウントを選択し、パブリック IP アドレスを有効にするか無効にするかなど、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。

Basic Settings

Project	Location
Project	Region
<div>OCCM-Dev</div>	<div>us-west1</div>
Service Account	Zone
<div>test</div>	<div>us-west1-a</div>
Select a Service Account that includes these permissions	VPC
	<div>default</div>
	Subnet
	<div>default</div>
	Public IP
	<div>Enable</div>

7. 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、プロキシの設定を指定します。

インターネットアクセスにプロキシが必要な場合は、データブローカーと同じサービスアカウントを Google Cloud で使用してプロキシを設定する必要があります。

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

このインスタンスの導入には、約 5 ～ 10 分かかります。進捗状況はBlueXPのコピーおよび同期サービスで監視できます。このサービスは、インスタンスが使用可能になると自動的に更新されます。

9. ウィザードのページに入力して、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導入し、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、追加の同期関係とともに使用できます。

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、BlueXPのコピーと同期では、データブローカーのサービスアカウントに使用する権限があるバケットから選択できます。デフォルトでは、これにはデータブローカーサービスアカウントと同じ `_PROJECT` に含まれるバケットが含まれます。ただし、必要な権限を指定した場合は、`_other_projects` 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 サービスをロードします。
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. 提供するロールを選択します [上記と同じ権限](#)。
7. [保存 (Save)] 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

BlueXPのコピーと同期では、以下の構成を使用してGoogle Cloudにデータブローカーが作成されます。

Node.jsとの互換性

v21.2.0

マシンのタイプ

N2 - 標準 -4

vCPU

4.

RAM

15 GB

オペレーティングシステム

Rocky Linux 9.0

ディスクのサイズとタイプ

20 GB HDD pd-standard

Linux ホストへのデータブローカーのインストール

新しいデータブローカーグループを作成する場合は、オンプレミスの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。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

Linux ホストの要件

- * Node.jsとの互換性* : v21.2.0
- * オペレーティング・システム * :

- CentOS 8.0および8.5

CentOS ストリームはサポートされていません。

- Red Hat Enterprise Linux 8.5、8.8、および8.9
- Rocky Linux 9
- Ubuntu Server 20.04 LTS の場合は
- SUSE Linux Enterprise Server 15 SP1

データ・ブローカーをインストールする前に'yum update'コマンドをホストで実行する必要があります

Red Hat Enterprise Linux システムは、Red Hat サブスクリプション管理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ソフトウェアをアップデートするためのリポジトリにアクセスできません。

- * RAM * : 16GB
- * CPU * : 4 コア
- * 空きディスク容量 * : 10 GB
- * SELinux * : 無効にすることをお勧めします ["SELinux"](#) ホスト。

SELinux では、データブローカーソフトウェアの更新をブロックし、通常運用に必要なエンドポイントにデータブローカーがアクセスできないようにするポリシーが適用されます。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

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。
- ファイルサーバが Linux ホストにエクスポートへのアクセスを許可している必要があります。
- AWS へのアウトバウンドトラフィック（データブローカーは常に Amazon SQS サービスと通信）を処理するために、Linux ホストでポート 443 が開いている必要があります。
- 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、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3つのコンポーネント間の時間差は5分を超えないようにしてください。

AWS へのアクセスを有効化

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場合は、Linux ホストで AWS にアクセスする準備をしておく必要があります。データブローカーをインストールする際、プログラム経由のアクセス権と特定の権限を持つ AWS ユーザに対して AWS キーを提供する必要があります。

手順

1. を使用して、IAM ポリシーを作成します ["ネットアップが提供するポリシーです"](#)

"AWS の手順を表示します。"

2. プログラムによるアクセス権を持つ IAM ユーザを作成します。

"AWS の手順を表示します。"

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ため、必ず AWS キーをコピーしてください。

Google Cloud へのアクセスを有効にします

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場合は、Google Cloud アクセス用の Linux ホストを準備しておく必要があります。データブローカーをインストールする場合、特定の権限を持つサービスアカウントにキーを提供する必要があります。

手順

1. Storage Admin の権限がない Google Cloud サービスアカウントを作成します。
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 の手順をご覧ください"

このファイルには、少なくとも「project_id」、「private_key」、および「client_email」というプロパティを含める必要があります。



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しています

Azure へのアクセスは、関係ごとに定義されます。そのためには、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します。

データブローカーのインストール

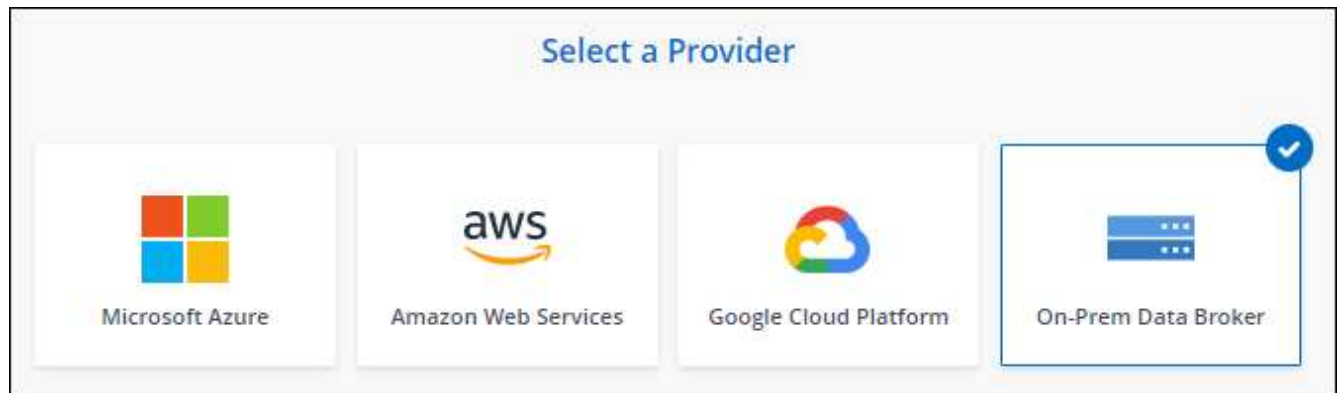
同期関係を作成するときに、Linux ホストにデータブローカーをインストールできます。

手順

1. [新しい同期の作成]*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、*[続行]*を選択します。

「* データブローカーグループ *」ページが表示されるまで、手順を完了します。

3. ページで、[データブローカーの作成]を選択し、[オンプレミスのデータブローカー]*を選択します。



このオプションには「*_オンプレミス_データブローカー*」というラベルが付けられていますが、オンプレミスまたはクラウド上の Linux ホストにも該当します。

4. データブローカーの名前を入力し、*[続行]*を選択します。

手順ページがすぐにロードされます。これらの手順に従う必要があります。インストーラ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。

5. 手順ページで次の手順を実行します。
 - 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として、*_プロキシなし*、*_プロキシサーバーを使用*、または*_認証付きプロキシサーバーを使用*を選択します。



ユーザはローカルユーザである必要があります。ドメインユーザはサポートされません。

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

次の手順では、使用可能な各インストールオプションの詳細を示します。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、手順ページを参照してください。

- d. インストーラをダウンロードします。

- プロキシなし：

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

- プロキシサーバを使用：

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

- プロキシサーバで認証を使用する：

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

URI

BlueXPのコピーと同期の手順ページにインストールファイルのURIが表示されます。プロンプトに従ってオンプレミスのデータブローカーを導入すると、このURIがロードされます。この

URI はリンクが動的に生成され、1 回しか使用できないため、ここでは繰り返し使用されません。 [BlueXPのコピーと同期からURIを取得するには、次の手順を実行します。](#)

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



以下に示す各コマンドには、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、手順ページを参照してください。

- プロキシ構成なし：

```
「 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 ファイル>`
```

- 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 ファイル> -h <proxy_host> -p
<proxy_port>`
```

- 認証を使用したプロキシ設定：

```
「 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> -u
<proxy_username> -w <proxy_password>
```

AWS キー

これらはユーザに適切なキーです 準備しておきます [次の手順を実行します](#)。AWS のキーはデータブローカーに格納され、オンプレミスネットワークやクラウドネットワークで実行されます。ネットアップでは、データブローカー以外でキーを使用していません。

JSON ファイル

この JSON ファイルにサービスアカウントが含まれています 準備しておく必要があるキー [次の手順を実行します](#)。

6. データブローカーが利用可能になったら、BlueXPのコピーと同期で*[続行]*を選択します。
7. ウィザードのページに入力して、新しい同期関係を作成します。

BlueXPのコピーと同期を使用

ソースとターゲットの間でデータを同期します

同期関係を作成する

同期関係を作成すると、BlueXPのコピーおよび同期サービスによって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、変更されたデータは 24 時間ごとに同期されます。

一部の種類の同期関係を作成する前に、まずBlueXPで作業環境を作成する必要があります。

特定のタイプの作業環境の同期関係を作成します

次のいずれかの同期関係を作成する場合は、最初に作業環境を作成または検出する必要があります。

- ONTAP 対応の Amazon FSX
- Azure NetApp Files の特長
- Cloud Volumes ONTAP
- オンプレミスの ONTAP クラスタ

手順

1. 作業環境を作成または検出します。
 - ["ONTAP 作業環境用の Amazon FSX を作成します"](#)
 - ["Azure NetApp Files をセットアップおよび検出しています"](#)
 - ["AWS での Cloud Volumes ONTAP の起動"](#)
 - ["Azure で Cloud Volumes ONTAP を起動します"](#)
 - ["Google Cloud で Cloud Volumes ONTAP を起動しています"](#)
 - ["既存の Cloud Volumes ONTAP システムの追加"](#)
 - ["ONTAP クラスタの検出"](#)
2. [キャンバス]*を選択します。
3. 上記のいずれかのタイプに一致する作業環境を選択してください。
4. [同期] の横のアクションメニューを選択します。



5. この場所から * データを同期 * または * この場所へのデータの同期 * を選択し、プロンプトに従って同期関係を設定します。

他のタイプの同期関係を作成します

ONTAP、Azure NetApp Files、Cloud Volumes ONTAP、オンプレミスの ONTAP クラスターで、Amazon FSX 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、次の手順を実行します。以下の手順は、NFS サーバから S3 バケットへの同期関係を設定する方法の例を示しています。

1. BlueXPで、* Sync *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。

次の手順では、NFS サーバから S3 バケットへの同期関係を作成する方法の例を示します。



3. NFS Server * ページで、AWS と同期する NFS サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
4. **[Data Broker Group]** 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、データブローカーソフトウェアを既存の Linux ホストに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 にデータブローカーを作成"](#)
- ["Azure でデータブローカーを作成"](#)
- ["Google Cloud でデータブローカーを作成"](#)
- ["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。



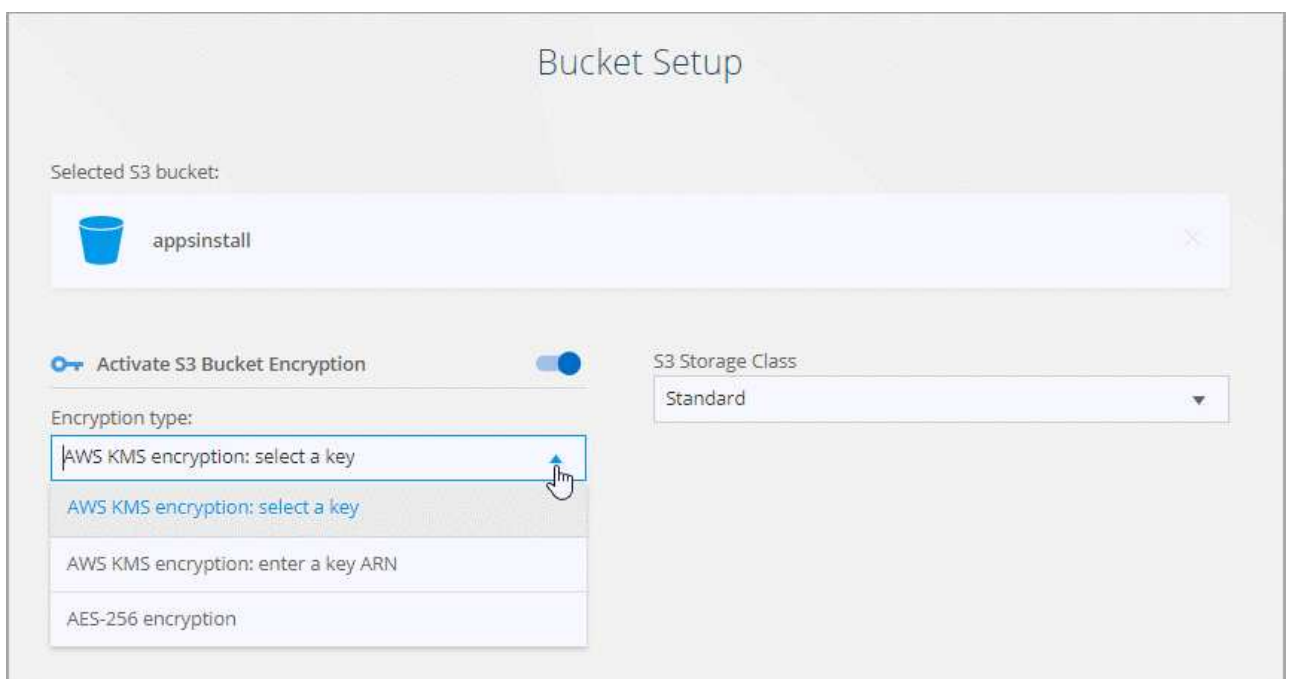
6. [Directories] ページで、最上位のディレクトリまたはサブディレクトリを選択します。

BlueXPの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 サーバ上の複数のディレクトリを同期する場合は、同期関係を作成してから同期関係を作成する必要があります。

7. 「* AWS S3 Bucket *」 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。
 - [リストに追加]*を選択して、AWSアカウントに関連付けられていないS3バケットを選択します。"[S3 バケットには特定の権限を適用する必要があります。](#)"。
8. [* Bucket Setup*] ページで、バケットを設定します。
- S3 バケットの暗号化を有効にするかどうかを選択し、AWS 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します。](#)"。



9. * ページで、ソースファイルとフォルダーを同期してターゲットの場所に保持する方法を定義します。

スケジュール

以降の同期に対して繰り返し実行する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。データを 1 分ごとに同期するように関係をスケジュールできます。

同期タイムアウト

指定した時間、時間、または日数内に同期が完了していない場合に、BlueXPのコピーと同期をキャンセルするかどうかを定義します。

通知

BlueXPのコピーと同期の通知をBlueXPの通知センターで受け取るかどうかを選択できます。データの同期が成功した場合、データの同期が失敗した場合、データの同期がキャンセルされた場合の通知を有効にできます。

再試行

BlueXPのコピーと同期がファイルの同期をスキップするまでに再試行する回数を定義します。

継続的同期

初回のデータ同期後、BlueXPのコピーと同期はソースのS3バケットまたはGoogle Cloud Storageバケットに対する変更をリスンし、ターゲットへの変更が発生したときに継続的に同期します。ソースを定期的に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場合、およびS3バケットまたはGoogle Cloud StorageからAzure BLOBストレージ、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、S3のデータを同期する場合にのみ使用できます。Azure Blob StorageからAzure Blob Storage、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、StorageGRID へのStorageGRID または。

この設定を有効にすると、他の機能に次のように影響します。

- 同期スケジュールが無効になっています。
- 次の設定が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、更新日。
- S3がソースの場合、サイズでのフィルタはコピーイベントに対して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）。
- 関係を作成したあとは、関係を高速化または削除する必要があります。同期の中止、設定の変更、レポートの表示はできません。

外部バケットとの間で継続的な同期関係を作成することができます。これを行うには、次の手順を実行します。

- 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 STOP ALL`

B. `sudo PM2 start all`

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の作成に使用したデータブローカーでは、プロジェクト内のバケットとの間に別の継続的同期関係を作成することはできません。

で比較してください

ファイルやディレクトリが変更されたかどうか、再同期が必要かどうかを判断する際に、BlueXPのコピーと同期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、BlueXPのコピーと同期ではパス、ファイルサイズ、ファイル名がチェックされてソースとターゲットが比較されます。変更がある場合は、それらのファイルとディレクトリが同期されます。

BlueXPのコピーと同期を有効または無効にして、次の属性を比較することができます。

- **mtime**: ファイルの最終変更時刻。この属性はディレクトリに対しては無効です。
- **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場合は、このオプションを有効にします。ユーザがソースのメタデータを変更した場合、BlueXPのコピーと同期は次回の同期でこのオブジェクトをコピーしますが、ユーザが（データ自体ではなく）ソースのタグを変更した場合、BlueXPのコピーと同期は次回の同期でオブジェクトをコピーしません。

関係の作成後にこのオプションを編集することはできません。

ターゲットにAzure BlobまたはS3互換エンドポイント（S3、StorageGRID、IBM Cloud Object Storage）を含む同期関係では、タグのコピーがサポートされます。

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せん。

- AWS S3
- Azure Blob の略

- Google クラウドストレージ
- IBM クラウドオブジェクトストレージ
- StorageGRID

最近変更されたファイル

スケジュールされた同期よりも前に最近変更されたファイルを除外するように選択します。

ソース上のファイルを削除します

BlueXPのコピーと同期でターゲットの場所にファイルがコピーされたあとに、ソースの場所からファイルを削除するように選択します。このオプションには、コピー後にソースファイルが削除されるため、データ損失のリスクも含まれます。

このオプションを有効にする場合は、データブローカーで local.json ファイルのパラメータ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ら、再起動します。 `pm2 restart all`。

ターゲット上のファイルを削除します

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が削除されることはありません。

ファイルの種類

各同期に含めるファイルタイプ（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からNFSへの関係でのみ使用できます。ユーザーは1つのスキャナプロセスと1つのスキャナ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します

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するには、ファイル拡張子を入力して*Enter*キーを押します。たとえば、「LOG_OR.log_」と入力すると、*.log ファイルが除外されます。複数の拡張子に区切り文字は必要ありません。次のビデオでは、簡単なデモを紹介しています。

▶ https://docs.netapp.com/ja-jp/bluexp-copy-sync//media/video_file_extensions.mp4 (video)



正規表現（正規表現）は、ワイルドカードやglob式とは異なります。この機能*only*は正規表現で動作します。

ディレクトリを除外します

同期から除外する正規表現またはディレクトリの名前またはフルパスを入力して*Enter*キーを押し、最大15個の正規表現またはディレクトリを指定します。デフォルトでは、.copy-Offload、.snapshot、~snapshotディレクトリが除外されます。



正規表現（正規表現）は、ワイルドカードやglob式とは異なります。この機能*only*は正規表現で動作します。

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、特定のサイズ範囲のファイルのみを同期するかを選択します。

変更日

最後に変更した日付、特定の日付以降に変更されたファイル、特定の日付より前、または期間に関係なく、すべてのファイルを選択します。

作成日

SMB サーバがソースの場合、この設定を使用すると、指定した日付の前、特定の日付の前、または特定の期間の間に作成されたファイルを同期できます。

[ACL] - アクセスコントロールリスト

関係の作成時または関係の作成後に設定を有効にして、ACLのみ、ファイルのみ、またはACLとファイルをSMBサーバからコピーします。

10. * Tags/Metadata* ページで、 S3 バケットに転送された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。

The screenshot shows the 'Relationship Tags' configuration page. At the top, there are navigation tabs: '<', 'AWS S3 Bucket', 'Settings', '6 Tags/Metadata', and '7 Review'. The main heading is 'Relationship Tags'. Below it, a message states: 'Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket. This enables you to search for the transferred files by using the tag values.' There are two radio buttons: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below these are two input fields: 'Tag Key' with a placeholder 'Up to 128 characters' and 'Tag Value' with a placeholder 'Up to 256 characters'. At the bottom left is a button '+ Add Relationship Tag' and at the bottom right is the text 'Optional Field | [Up to 5]'.



この機能は、StorageGRID と IBM Cloud Object Storage にデータを同期する場合にも使用できます。Azure と Google Cloud Storage では、メタデータオプションのみを使用できます。

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 *

BlueXPのコピーと同期で、ソースとターゲット間のデータの同期が開始されます。

BlueXPの分類から同期関係を作成

BlueXPのコピーと同期はBlueXPの分類機能に統合されています。BlueXPの分類から、BlueXPの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。

BlueXPの分類からデータの同期を開始すると、すべてのソース情報が1つの手順で格納され、重要な詳細情報をいくつか入力するだけで済みます。その後、新しい同期関係の作成先を選択します。

"BlueXPの分類から同期関係を開始する方法"。

SMB 共有から ACL をコピーする

BlueXPのコピーと同期では、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Access Control List（ACL；アクセス制御リスト）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。

選択肢

- ACLを自動的にコピーするようにBlueXPのコピーと同期を設定
- SMB 共有間で ACL を手動でコピーします

BlueXPのコピーと同期を設定してACLをコピー

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をコピーするには、関係の作成時または作成後に設定を有効にします。

作業を開始する前に

この機能は、_any_type のデータブローカー（AWS、Azure、Google Cloud Platform、オンプレミスのデータブローカー）と連携します。オンプレミスのデータブローカーを実行できます ["サポートされているオペレーティングシステム"](#)。

新しい関係の手順

1. BlueXPのコピーと同期で、*[Create New Sync]*を選択します。
2. SMBサーバ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。
3. [* SMB サーバー *] ページで、次の操作を行います。
 - a. 新しいSMBサーバを入力するか、既存のサーバを選択して*[続行]*を選択します。
 - b. SMB サーバのクレデンシャルを入力します。
 - c. ファイルのみをコピー、*ACLのみをコピー*、または*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。

Select an SMB Source

SMB Server Version : 2.1

Selected SMB Server:

210.10.10.10 [Change Server](#)

Define SMB Credentials:

User Name Password Domain (Optional)

user1 *****

ACL - Access Control List

Copy only files

Notice: Copying ACLs can affect sync performance. You can change this setting after you create the relationship.

Attention: If the sync relationship includes Cloud Volumes ONTAP or an on-prem ONTAP cluster and you selected NFSv4 or later, then you'll need to enable NFSv4 ACLs on the ONTAP system. This is required to copy the ACLs.

4. 残りのプロンプトに従って、同期関係を作成します。

ACL を SMB からオブジェクトストレージにコピーする際、ターゲットに応じて、オブジェクトのタグまたはオブジェクトのメタデータに ACL をコピーするかを選択できます。Azure と Google Cloud Storage では、メタデータオプションのみを使用できます。

次のスクリーンショットは、このオプションを選択できる手順の例を示しています。

Relationship Metadata

Cloud Sync assigns the relationship metadata to all of the files transferred to the S3 bucket.

☐ Save on Object's Tags
 ☒ Save On Object's Metadata

Metadata Key: Up to 128 characters

Metadata Value: Up to 256 characters

Optional Field | [Up to 5]

既存の関係に対する手順

1. 同期関係にカーソルを合わせ、操作メニューを選択します。
2. [設定]*を選択します。
3. ファイルのみをコピー、* ACLのみをコピー*、または*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. [設定の保存]*を選択します。

結果

BlueXPのコピーと同期では、データの同期時にソースとターゲットの間のACLが保持されます。

SMB共有間でACLを手動でコピーします

Windows の Robocopy コマンドを使用すると、SMB 共有間で ACL を手動で保存できます。

手順

1. 両方の SMB 共有へのフルアクセス権を持つ 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. BlueXPのコピーと同期から、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. データの同期が完了したら、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]"
```

UNC 形式を使用して、source_or_target_ と target の両方を指定する必要があります。たとえば、\\<server>\<share>\<path> と入力します

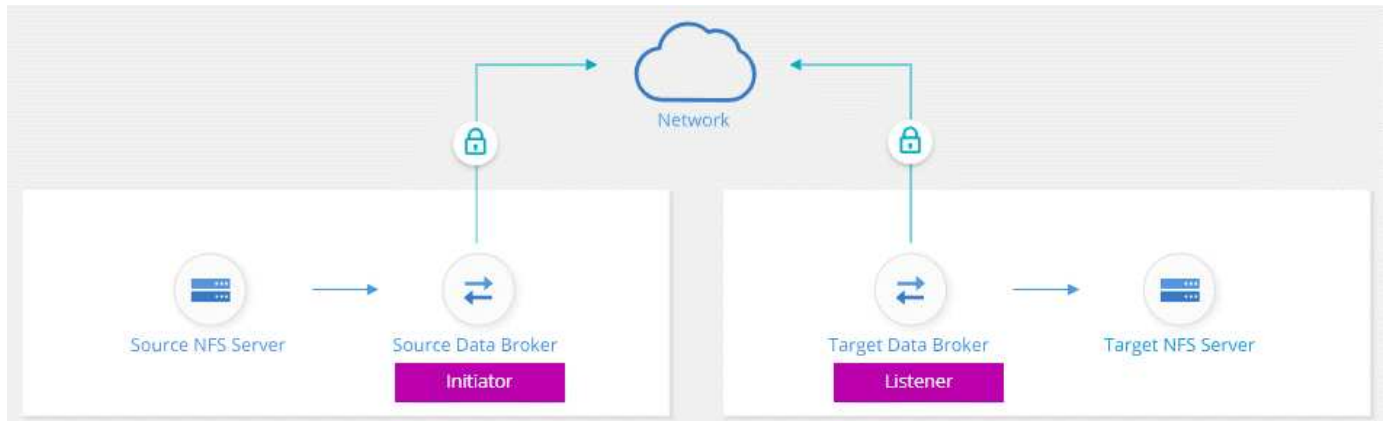
転送中のデータ暗号化を使用した **NFS** データの同期

厳格なセキュリティポリシーを適用している場合は、転送中データの暗号化を使用して NFS データを同期できます。この機能は、NFS サーバから別の NFS サーバ、および Azure NetApp Files から Azure NetApp Files へサポートされます。

たとえば、異なるネットワークにある 2 つの NFS サーバ間でデータを同期できます。また、サブネットやリジョン間で Azure NetApp Files 上のデータをセキュアに転送しなければならない場合もあります。

データインフラ暗号化の仕組み

データ転送中の暗号化では、2 つのデータブローカー間でネットワークを介して送信される NFS データが暗号化されます。次の図は、2 つの NFS サーバと 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は、*initiator* として機能します。データを同期するときは、接続要求をもう 1 つのデータブローカー（つまり *listener*）に送信します。そのデータブローカーは、ポート 443 で要求をリスンします。必要に応じて別のポートを使用できますが、そのポートが別のサービスで使用されていないことを確認してください。

たとえば、オンプレミスの NFS サーバからクラウドベースの NFS サーバにデータを同期する場合、接続要求を受信するデータブローカーと送信するデータブローカーを選択できます。

転送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 を使用してソースのデータを暗号化します。
3. 次に、ネットワーク経由でデータをターゲットデータブローカーに送信します。
4. ターゲットのデータブローカーは、ターゲットに送信する前にデータを復号化します。
5. 最初のコピーの後、変更されたデータは 24 時間ごとに同期されます。同期するデータがある場合は、イニシエータが他のデータブローカーとの暗号化された接続を開いてプロセスが開始されます。

データをより頻繁に同期する場合は、["スケジュールは関係の作成後に変更することができます"](#)。

サポートされている **NFS** のバージョン

- NFS サーバでは、データ転送時の暗号化が NFS バージョン 3、4.0、4.1、4.2 でサポートされていま

す。

- Azure NetApp Files では、NFS バージョン 3 および 4.1 でデータ転送時の暗号化がサポートされます。

プロキシサーバの制限事項

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、プロキシサーバ経由でルーティングすることはできません。

開始するには、何が必要ですか

次のものを用意してください。

- に対応した 2 台の NFS サーバ ["移行元と移行先の要件"](#) または、2 つのサブネットまたはリージョンの Azure NetApp Files。
- サーバの 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ロケーション。

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、_NET_DATA ブローカ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、データブローカーが 1 つだけである必要があります。グループ内の複数のデータブローカーは、暗号化された同期関係ではサポートされません。

データブローカーをまだ導入していない場合は、データブローカーの要件を確認します。厳格なセキュリティポリシーがあるため、ポート 443 およびからの発信トラフィックを含むネットワーク要件を確認してください ["インターネットエンドポイント"](#) データブローカーの連絡先。

- ["AWS のインストールを確認します"](#)
- ["Azure のインストールを確認します"](#)
- ["Google Cloud のインストール状況を確認します"](#)
- ["Linux ホストのインストールを確認します"](#)

転送中のデータ暗号化を使用した NFS データの同期

2 つの NFS サーバ間または Azure NetApp Files 間で新しい同期関係を作成し、転送中の暗号化オプションを有効にして、画面の指示に従います。

手順

1. [新しい同期の作成]*を選択します。
2. NFS サーバ* 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て、* はい * を選択して転送中のデータ暗号化を有効にします。
3. プロンプトに従って関係を作成します。
 - a. * NFS サーバ * / * Azure NetApp Files * : NFS のバージョンを選択し、新しい NFS ソースを指定するか、既存のサーバを選択します。
 - b. * データブローカー機能の定義 *: ポート上での接続要求に対して 'どのデータ・ブローカ・リスン _ がどのデータ・ブローカ・リスン _ を実行するか' およびどのデータ・ブローカが接続を開始するか

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。

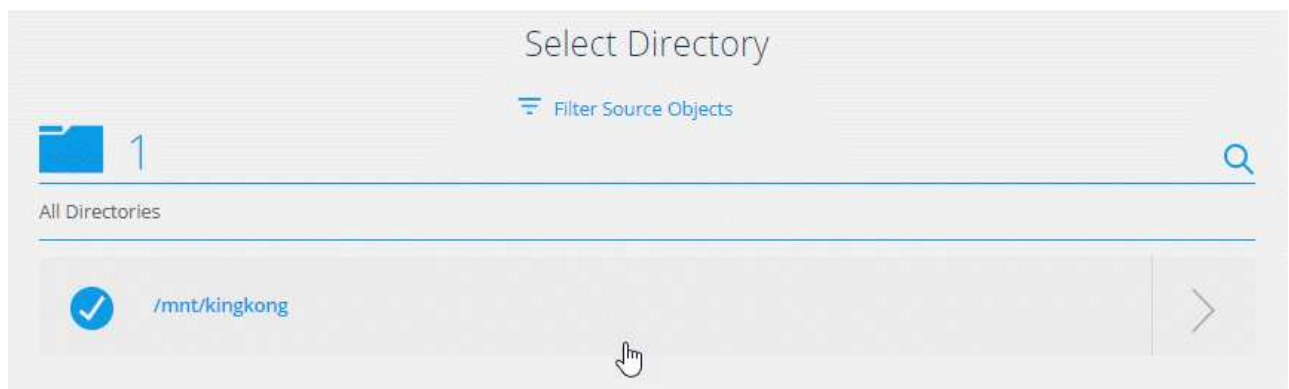
- c. * データブローカー * : 新しいソースデータブローカーを追加するか、既存のデータブローカーを選択するよう求められます。

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、データブローカーが 1 つだけである必要があります。グループ内の複数のデータブローカーは、暗号化された同期関係で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、BlueXPのコピーと同期によってインストール手順が表示されます。クラウドにデータブローカーを導入したり、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。

- 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。

[ソースオブジェクトのフィルタ]*を選択して、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する設定を変更します。




オプションを選択するオプションを示すスクリーンショット。"]

- 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 * : 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するよう求められます。


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は、新しいデータブローカーである必要があります。

ターゲットの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目してください。


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform

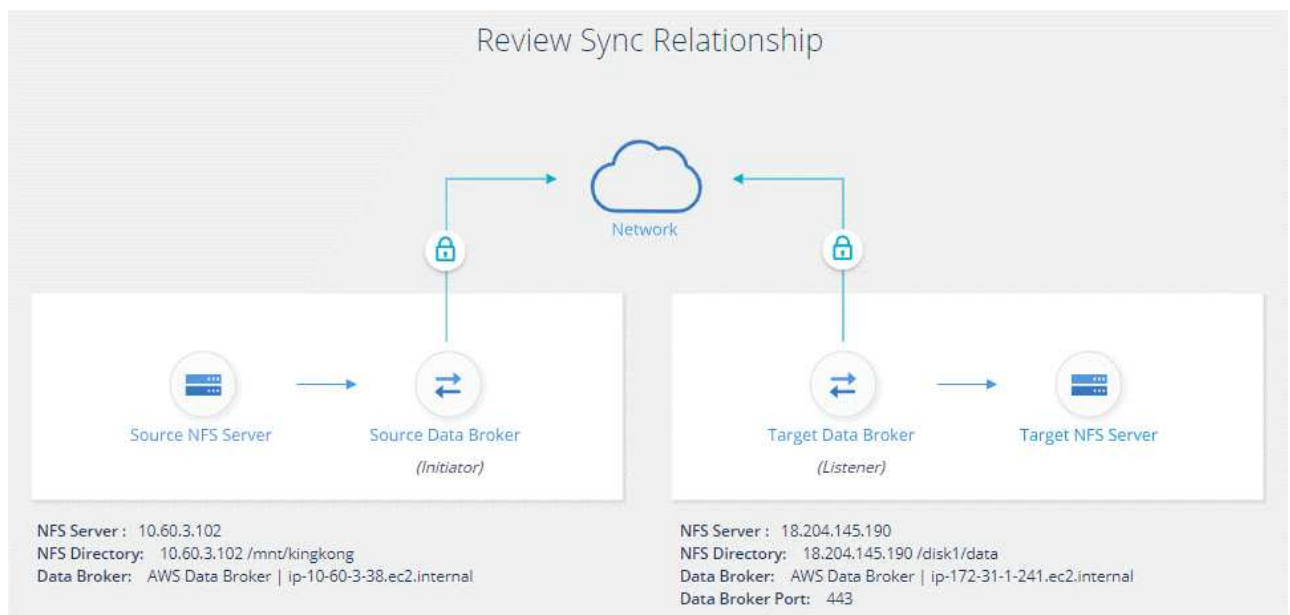


On-Prem Data Broker

Data Broker Name

Port

- a. * ターゲットディレクトリ * : トップレベルの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を作成します。
- b. * 設定 * : 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。
- 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

BlueXPのコピーと同期が新しい同期関係の作成を開始します。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。

外部の橋本社ボルトを使用するように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のクレデンシャルを必要とする同期関係を作成する場合は、BlueXPのコピーと同期のユーザインターフェイスまたはAPIでクレデンシャルを指定する必要があります。別の方法として、外部の橋本社ボルトから直接ク

レデンシヤル（または *secrets*）にアクセスするようにデータブローカーグループを設定する方法もあります。

この機能は、Amazon S3、Azure、Google Cloudのクレデンシヤルを必要とする同期関係を備えたBlueXPのコピーおよび同期APIでサポートされます。

1

ボルトを準備します

URL を設定して、データブローカーグループにクレデンシヤルを提供するようにヴォールトを準備します。ボルトのシークレットの 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を準備

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、外部ボルトからクレデンシヤルを取得するようにデータブローカーグループを準備します。

3

API を使用して同期関係を作成してください

すべての設定が完了したら、API 呼び出しを送信して、ヴォ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。

ヴォールトを準備しています

BlueXPのコピーを提供し、ボルト内のシークレットのURLと同期する必要があります。URL を設定してボルトを準備します。作成する同期関係の各ソースとターゲットのクレデンシヤルへの 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`」を指定します

パス

シークレットへのプレフィックスパス。この値は、お客様に固有の任意の値にすることができます。

リクエスト 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は、API POST 要求のいずれかのヘッダーに 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

定義されている次のいずれかのプロトコル ["v2 以降の関係に関するドキュメント"](#)：S3、Azure、GCP（それぞれ大文字で入力する必要があります）。

Creds（作成）

URL の末尾は *creds.* にする必要があります。

例

次の例は、シークレットへの URL を示しています。

ソースクレデンシャルの完全な URL とパスの例

\ <http://example.vault.com:8200/my-path/all-secrets/hb312vdsr2/S3Creds>

この例のように、プレフィックスパスは `/my-path/all-secrets/` で、要求 ID は `_hb312vdsr2_` で、ソースエンドポイントは S3 です。

ターゲットクレデンシャルの完全な 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を準備しています

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、外部ボルトからクレデンシャルを取得するようにデータブローカーグループを準備します。

手順

1. グループ内のデータブローカーへの SSH 接続
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-m積分 .hashicorp_as` の下に `config` パラメータフィールドを設定します。

有効

- 有効な値は、`true` または `false` です
- `type` : ブール値
- デフォルト値: `false`
- `true` : データブローカーは、社内の外部の橋本社から機密情報を入手します
- `false` : データブローカーのクレデンシャルがローカルボルトに格納されます

URL

- 文字列を入力します
- 値: 外部ボルトの URL

パス

- 文字列を入力します
- 値: クレデンシャルを使用してシークレットへのプレフィックスパスを指定します

拒否 - 承認されていません

- データブローカーで権限のないことを拒否するかどうかを指定します 外部ボルト
- `type` : ブール値
- デフォルト: `false`

`auth-method` を指定します

- データブローカーが外部ボルトのクレデンシャルにアクセスする際に使用する認証方式

- 文字列を入力します
- 有効な値は「AWS- IAM」 / 「role-app」 / 「GCP-IAM」です。

ロール名

- 文字列を入力します
- ロール名（AWS- IAM または GCP-IAM を使用している場合）

Secretid&rootid

- タイプ：string （app-role を使用する場合）

ネームスペース

- 文字列を入力します
- ネームスペース（必要に応じて X-Vault - 名前空間ヘッダー）

4. グループ内の他のすべてのデータブローカーについて、上記の手順を繰り返します。

AWS ロール認証の例

```
{
  "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 認証を使用する場合に権限を設定します

_GCP-AM_authentication メソッド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 権限要件の詳細については、こちらをご覧ください"。

ヴォールトのシークレットを使用して、新しい同期関係を作成します

すべての設定が完了したら、API 呼び出しを送信して、ヴォ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。

BlueXPのコピーを使用して関係をPOSTし、REST APIを同期

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BlueXPアカウントIDを取得するには ["のドキュメントのこのページを参照してください"](#)。
- 投稿関係の本文を作成するには、 ["relationships-v2 API 呼び出しを参照してください"](#)。

例

POST 要求の例：

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"
    }
  }
}
```

無料トライアルの終了後に同期関係の料金を支払う

14 日間の無料トライアル終了後に、同期関係の料金を支払う方法は 2 通りあります。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払いのいずれかを購読することです。2 つ目の選択肢は、ネットアップ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。

Marketplace サブスクリプションを使用して、ネットアップからライセンスを使用することもできます。たとえば、25 の同期関係がある場合は、ライセンスを使用して最初の 20 の同期関係に料金を支払い、残りの 5 つの同期関係を持つ 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は、こちらをご覧ください。](#)"。

無償トライアルの終了後すぐに支払いを行わないと、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、ライセンスを登録または入力するまでは変更を加えることはできません。

ライセンスの管理には、BlueXPのコピーと同期、または該当するWebサイトを使用する必要があります。デジタルウォレットを使用することはできません*。

[AWS] AWSからサブスクライブしています

AWS を使用すると、従量課金制または年払いが可能です。

従量課金制の手順

1. [同期]>[ライセンス]*を選択します。
2. 「*AWS*」を選択します
3. を選択し、[続行]*を選択します。
4. AWS Marketplaceから登録し、BlueXPのコピー&同期サービスに再度ログインして登録を完了します。

次のビデオは、プロセスを示しています。

▶ https://docs.netapp.com/ja-jp/bluexp-copy-sync//media/video_cloud_sync_registering.mp4 (video)

年間の支払い手順

1. "[AWS Marketplace ページに移動します。](#)"。
2. [購読を続行する]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から購読しています

Azure では、従量課金制または年間の支払いが可能です。

必要なもの

関連するサブスクリプションの投稿者または所有者権限を持つ Azure ユーザーアカウント。

手順

1. [同期]>[ライセンス]*を選択します。
2. 「* Azure *」を選択します。
3. を選択し、[続行]*を選択します。
4. 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。

「毎月 *」を選択すると、時間単位で支払います。または、「毎年」を選択すると、前払いした 1 年分の料金が支払われます。

5. 導入が完了したら、通知ポップアップでSaaSリソースの名前を選択します。
6. BlueXPのコピーと同期に戻るには、[アカウントの設定]*を選択します。

次のビデオは、プロセスを示しています。

▶ https://docs.netapp.com/ja-jp/bluexp-copy-sync//media/video_cloud_sync_registering_azure.mp4

(video)

[[licenses] ネットアップからライセンスを購入し、BlueXPのコピーと同期に追加します

同期関係の料金を事前に支払うには、1つ以上のライセンスを購入してBlueXPのコピーおよび同期サービスに追加する必要があります。

必要なもの

ライセンスのシリアル番号、およびライセンスが関連付けられているネットアップサポートサイトのアカウントのユーザ名とパスワードが必要です。

手順

1. mailto : ng-cloudsync-contact@netapp.com ? subject= Cloud %20Sync%20Service%20-%20BYOL %20License%20Purchase%20Request までにライセンスを購入してください。 [Contacting NetApp]。
2. BlueXPで、*[同期]>[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ます。
 - b. 追加するライセンスに関連付けられているネットアップサポートサイトのアカウントを選択します。
 - アカウントがBlueXPにすで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、[Add NSS Credentials]*を選択し、ユーザ名とパスワードを入力して[Register]*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。

ライセンスの更新

ネットアップから購入したBlueXPのコピーと同期のライセンスを延長した場合、BlueXPのコピーと同期で新しい有効期限が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。ライセンスの管理には、BlueXPのコピーと同期、または該当するWebサイトを使用する必要があります。デジタルウォレットを使用することはできません*。

手順

1. BlueXPで、*[同期]>[ライセンス]*を選択します。
2. [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ます。
 - b. 追加するライセンスに関連付けられているネットアップサポートサイトのアカウントを選択します。
 - c. 「* 追加」を選択します。

結果

BlueXPの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に更新されます。


同期関係の管理

データの即時同期や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します

スケジュールされた次回の同期を待つのではなく、ボタンを押すと、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. [ダッシュボード]*で、同期関係に移動してを選択します 
2. を選択し、[同期]*を選択して確定します。

結果

BlueXPのコピーと同期によって、関係のデータ同期プロセスが開始されます。

同期のパフォーマンスを高速化

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で、同期関係のパフォーマンスを向上できます。追加のデータブローカーには、_NET_DATA ブローカーを指定する必要があります。

この仕組み


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、グループに追加した新しいデータブローカーを使用することで、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

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 に追加するため、関係 1 のパフォーマンスを高速化したいと考えていますグループ A でも同期関係 3 が管理されるため、関係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]*で、同期関係に移動してを選択します 
3. [高速化]*を選択します。
4. プロンプトに従って、新しいデータブローカーを作成します。

結果

BlueXPの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を高速化する必要があります。

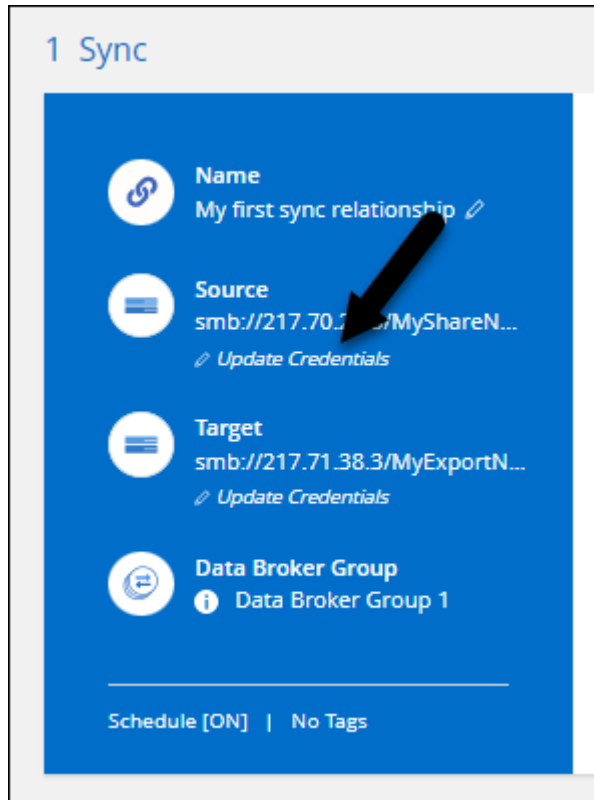
UpdateCredentials

データブローカーを、既存の同期関係にあるソースまたはターゲットの最新のクレデンシャルで更新できます。クレデンシャルの更新は、セキュリティポリシーで定期的にクレデンシャルの更新が要求される場合に役立ちます。

クレデンシャルの更新は、BlueXPのコピーと同期に必要な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）でサポートされます。

手順

1. で、クレデンシャルが必要な同期関係に移動し、[クレデンシャルの更新]*を選択します。



ページの [資格情報の更新] オプションを示すスクリーンショット。"]

2. クレデンシャルを入力し、*[更新]*を選択します。

SMB サーバに関する注意：新しいドメインの場合は、クレデンシャルを更新するときにドメイン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。

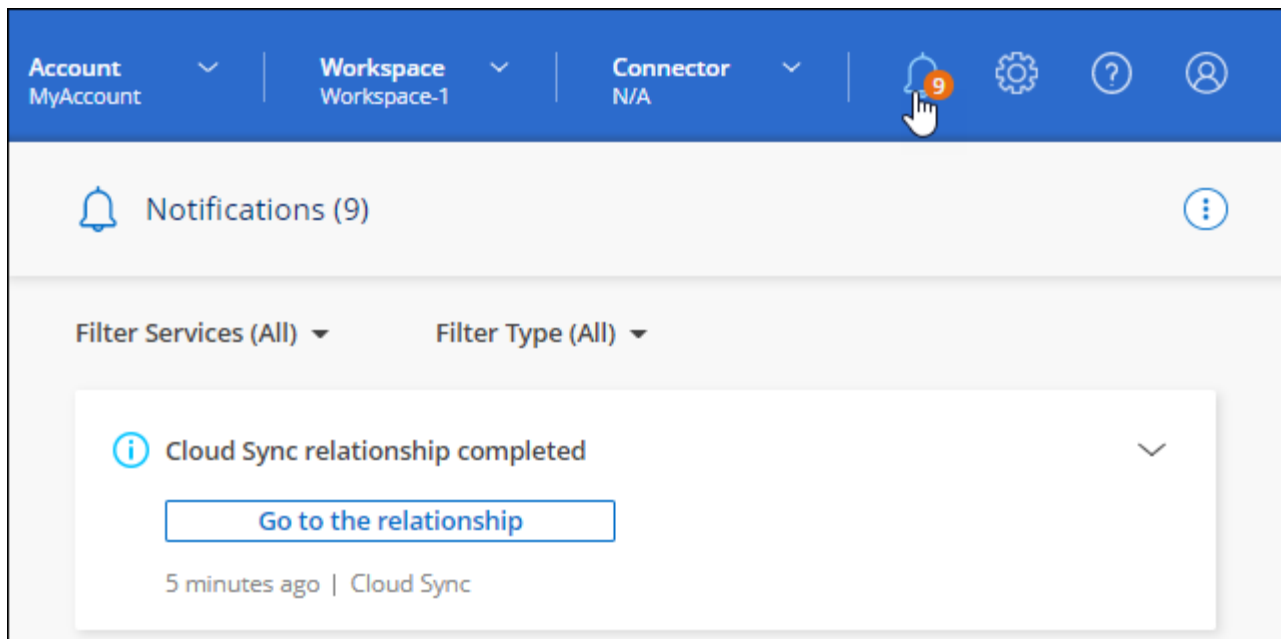
同期関係の作成時にドメインを入力したが、クレデンシャルの更新時に新しいドメインを入力しなかった場合、BlueXPのコピーと同期では指定した元のドメインが引き続き使用されます。

結果

BlueXPのコピーと同期により、データブローカーのクレデンシャルが更新されます。データブローカーがデータ同期用に更新されたクレデンシャルを使用して起動するまで、10分程度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]*設定を使用すると、BlueXPのコピーと同期の通知をBlueXPの通知センターで受け取るかどうかを選択できます。データの同期が成功した場合、データの同期が失敗した場合、データの同期がキャンセルされた場合の通知を有効にできます。



また、E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]*で、同期関係に移動してを選択します 
 - b. [設定]*を選択します。
 - c. 通知を有効にする*。
 - d. [設定の保存]*を選択します。
2. Eメールで通知を受信する場合は、アラートと通知を設定します。
 - a. [設定]>[アラートと通知の設定]*を選択します。
 - b. ユーザまたは複数のユーザを選択し、「*情報」通知タイプを選択します。
 - c. *適用*を選択します。

結果

BlueXPのコピーと同期の通知がBlueXPの通知センターで受信されるようになりました。このオプションを設定している場合は、いくつかの通知がEメールで送信されます。

同期関係の設定を変更します

ソースファイルとフォルダの同期方法とターゲットの場所での保持方法を定義する設定を変更します。

1. [ダッシュボード]*で、同期関係に移動してを選択します 
2. [設定]*を選択します。
3. 設定を変更します。

General

Schedule

ON | Every 1 Day

▼

Retries

Retry 3 times before skipping file

▼

Files and Directories

Compare By

The following attributes (and size): uid, gid, mode, mtime

▼

Recently Modified Files

Exclude files that are modified up to 30 Seconds before a scheduled sync

▼

Delete Files On Source

Never delete files from the source location

▼

Delete Files On Target

Never delete files from the target location

▼

File Types

Include All: Files, Directories, Symbolic Links

▼

Exclude File Extensions

None

▼

File Size

All

▼

Date Modified

All

▼

Date Created

All

▼

ACL - Access Control List

Inactive

▼

Reset to defaults

[削除ソース] 各設定の簡単な説明を次に示します。

スケジュール

以降の同期に対して繰り返し実行する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。データを 1 分ごとに同期するように関係をスケジュールできます。

同期タイムアウト

指定した時間、時間、または日数内に同期が完了していない場合に、BlueXPのコピーと同期をキャンセルするかどうかを定義します。

通知

BlueXPのコピーと同期の通知をBlueXPの通知センターで受け取るかどうかを選択できます。データの

同期が成功した場合、データの同期が失敗した場合、データの同期がキャンセルされた場合の通知を有効にできます。

の通知を受信する場合は

再試行

BlueXPのコピーと同期がファイルの同期をスキップするまでに再試行する回数を定義します。

で比較してください

ファイルやディレクトリが変更されたかどうか、再同期が必要かどうかを判断する際に、BlueXPのコピーと同期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、BlueXPのコピーと同期ではパス、ファイルサイズ、ファイル名がチェックされてソースとターゲットが比較されます。変更がある場合は、それらのファイルとディレクトリが同期されます。

BlueXPのコピーと同期を有効または無効にして、次の属性を比較することができます。

- **mtime**: ファイルの最終変更時刻。この属性はディレクトリに対しては無効です。
- **uid**、**gid** *、および *** mode** : Linux の権限フラグ。

オブジェクトのコピー

関係の作成後に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よりも前に最近変更されたファイルを除外するように選択します。

ソース上のファイルを削除します

BlueXPのコピーと同期でターゲットの場所にファイルがコピーされたあとに、ソースの場所からファイルを削除するように選択します。このオプションには、コピー後にソースファイルが削除されるため、データ損失のリスクも含まれます。

このオプションを有効にする場合は、データブローカーで local.json ファイルのパラメータ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ら、再起動します。 `pm2 restart all`。

ターゲット上のファイルを削除します

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が削除されることはありません。

ファイルの種類

各同期に含めるファイルタイプ（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からNFSへの関係でのみ使用できます。ユーザーは1つのスキャナプロセスと1つのスキャナ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します

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するには、ファイル拡張子を入力して*Enter*キーを押します。たとえば、「LOG_OR.log_」と入力すると、*.log ファイルが除外されます。複数の拡張子に区切り文字は必要ありません。次のビデオでは、簡単なデモを紹介しています。

▶ https://docs.netapp.com/ja-jp/bluexp-copy-sync//media/video_file_extensions.mp4 (video)



正規表現（正規表現）は、ワイルドカードやglob式とは異なります。この機能*only*は正規表現で動作します。

ディレクトリを除外します

同期から除外する正規表現またはディレクトリの名前またはフルパスを入力して*Enter*キーを押し、最大15個の正規表現またはディレクトリを指定します。デフォルトでは、.copy-Offload、.snapshot、~snapshotディレクトリが除外されます。



正規表現（正規表現）は、ワイルドカードやglob式とは異なります。この機能*only*は正規表現で動作します。

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、特定のサイズ範囲のファイルのみを同期するかを選択します。

変更日

最後に変更した日付、特定の日付以降に変更されたファイル、特定の日付より前、または期間に関係なく、すべてのファイルを選択します。

作成日

SMB サーバがソースの場合、この設定を使用すると、指定した日付の前、特定の日付の前、または特定の期間の間に作成されたファイルを同期できます。

[ACL] - アクセスコントロールリスト

関係の作成時または関係の作成後に設定を有効にして、ACLのみ、ファイルのみ、またはACLとファイルをSMBサーバからコピーします。

4. [設定の保存]*を選択します。

結果


BlueXPのコピーと同期は、新しい設定を使用して同期関係を変更します。

関係を削除します

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が削除されることもありません。

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]*で、同期関係に移動してを選択します 
2. を選択し、もう一度[削除]*を選択して確定します。

結果

BlueXPのコピーと同期によって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. [Dashboard]*で、[Create New Sync]ボタンに移動し、を選択します 
2. 削除する同期関係を選択し、[削除]*を選択し、[削除]*をもう一度選択して確認します。

結果

BlueXPのコピーと同期によって同期関係が削除されます。

データブローカーグループの管理

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、少なくとも1つのデータブローカーがグループに必要です。グループに新しいデータブローカーを追加し、グループに関する情報を表示するなどして、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を向上させることができます。

グループは複数の関係を管理できます

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て。

- 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

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 に追加するため、関係 1 のパフォーマンスを高速化したいと考えていますグループ A でも同期関係 3 が管理されるため、関係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、1 つ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、データブローカーをグループに追加することで、同期パフォーマンスを高速化できます。ただし、まず、同期の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いつ行われるかを確認する方法については、こちらをご覧ください](#) は必須です"。

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、次のことを推奨します。

- SSH で X11 転送を許可しないでください
- SSH では、TCP 接続の転送を許可しないでください
- SSH ではトンネルを許可しないでください
- SSH では、クライアント環境変数を受け入れないでください

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止するのに役立ちます。

新しいデータブローカーをグループに追加

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場合

"[作成時に新しいデータブローカーを作成する方法について説明します](#) 同期関係"。

- [データブローカーの管理] ページで*[新しいデータブローカーの追加]*を選択すると、新しいグループにデータブローカーが作成されます。
- 新しいを作成して、[データブローカーの管理 (Manage Data Brokers)] ページからアクセスします 既存のグループのデータブローカー

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であるか、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、そのグループに AWS データブローカーまたはオンプレミスの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、同じタイプのデータブローカーではないため、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. [同期]>[データブローカーの管理]*を選択します。
2. [新しいデータブローカーの追加]*を選択します。

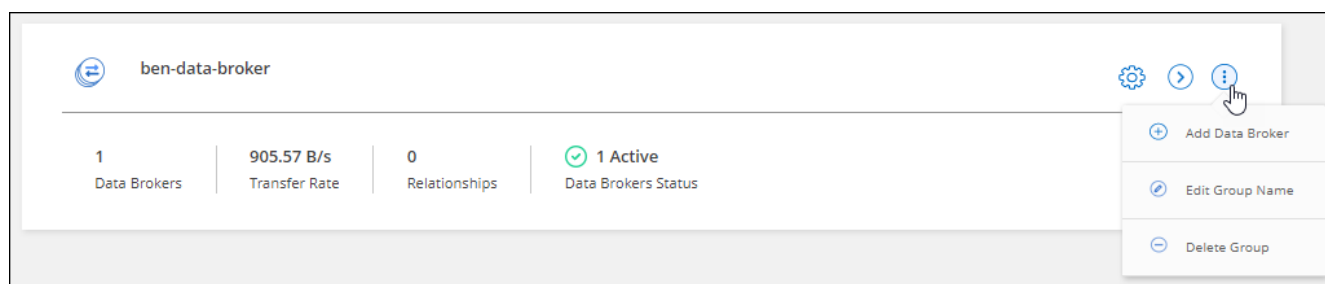
3. プロンプトに従ってデータブローカーを作成します。

ヘルプについては、次のページを参照してください。

- ["AWS にデータブローカーを作成"](#)
- ["Azure でデータブローカーを作成"](#)
- ["Google Cloud でデータブローカーを作成"](#)
- ["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. [同期]>[データブローカーの管理]*を選択します。
2. 操作メニューを選択し、*[データブローカーの追加]*を選択します。



3. プロンプトに従って、グループ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。

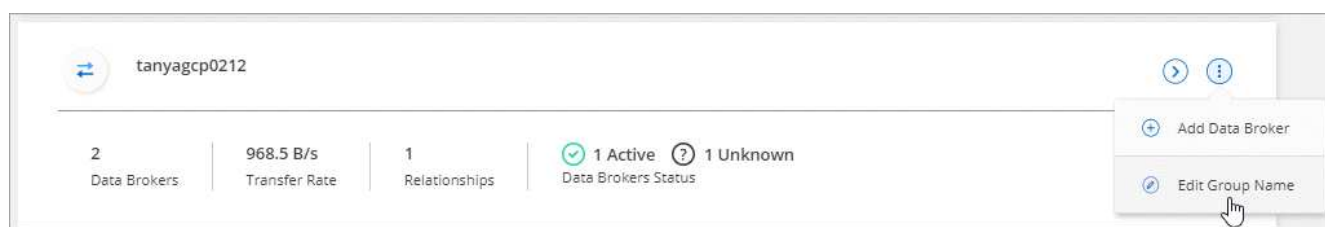
- ["AWS にデータブローカーを作成"](#)
- ["Azure でデータブローカーを作成"](#)
- ["Google Cloud でデータブローカーを作成"](#)
- ["Linux ホストへのデータブローカーのインストール"](#)

グループの名前を編集します

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. [同期]>[データブローカーの管理]*を選択します。
2. 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。



3. 新しい名前を入力し、*[保存]*を選択します。

結果

BlueXPの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。

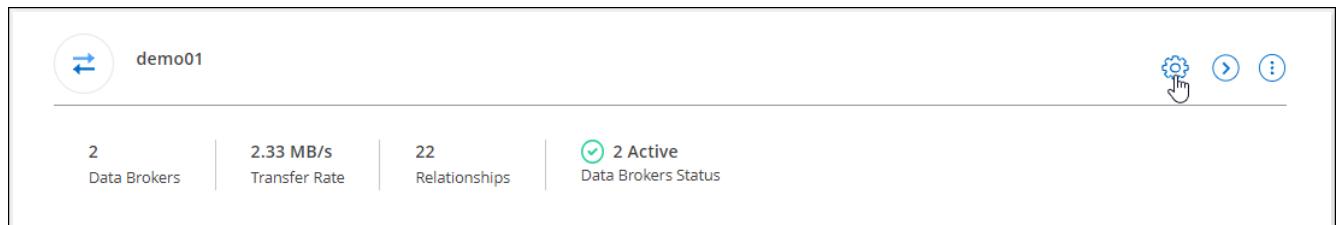
ユニファイド構成をセットアップする

同期プロセス中に同期関係でエラーが発生した場合は、データブローカーグループの同時実行を統合すると、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、転送速度が遅くなるため、パフォーマンスに影響する可能性があります。

自分で設定を変更することはお勧めしません。設定を変更するタイミングと変更方法については、ネットアップに相談してください。

手順

1. [データブローカーの管理]*を選択します。
2. データブローカーグループの[Settings]アイコンを選択します。



3. 必要に応じて設定を変更し、* Unify Configuration *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。
- この変更が行われ、BlueXPのコピーと同期のインターフェイスに表示されるまで、1分ほどかかることがあります。
- データブローカーが実行されていない場合、BlueXPのコピーと同期は通信できないため、データブローカーの設定は変更されません。データブローカーが再起動すると設定が変更されます。
- ユニファイド構成を設定すると、新しいデータブローカーでは自動的に新しい構成が使用されます。

データブローカーをグループ間で移動

ターゲットの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、データブローカーで同期関係が管理されなくなった場合、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。

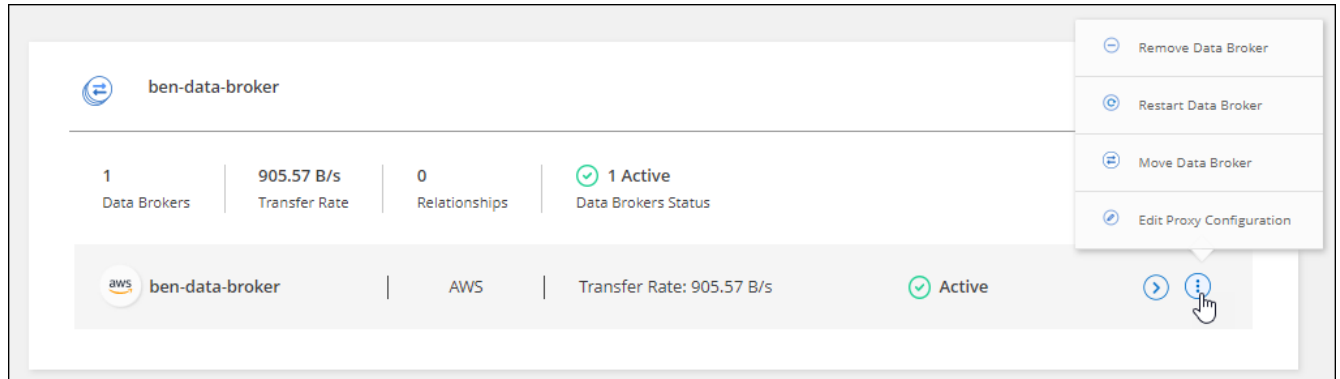
制限

- データブローカーグループが同期関係を管理していて、グループにデータブローカーが 1 つしかない場合、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との間でデータブローカーを移動することはできません。
- 現在導入中のデータブローカーは移動できません。

手順

1. [同期]>[データブローカーの管理]*を選択します。
2. 選択するオプション  をクリックして、グループ内のデータブローカーのリストを展開します。
3. データブローカーの操作メニューを選択し、*[データブローカーの移動]*を選択します。



4. 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てください。
5. [移動]*を選択します。


結果

BlueXPのコピーと同期により、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前のグループに他のデータブローカーがない場合は、BlueXPのコピーと同期によってデータブローカーが削除されます。

プロキシ設定を更新します

データブローカーのプロキシ設定を更新するには、新しいプロキシ設定に関する詳細を追加するか、既存のプロキシ設定を編集します。

手順

1. [同期]>[データブローカーの管理]*を選択します。
2. 選択するオプション  をクリックして、グループ内のデータブローカーのリストを展開します。
3. データブローカーの操作メニューを選択し、*[プロキシ設定の編集]*を選択します。
4. プロキシに関する詳細を指定します。ホスト名、ポート番号、ユーザ名、パスワードです。
5. 「* Update *」を選択します。

結果

BlueXPのコピーと同期により、データブローカーが更新され、プロキシ設定を使用してインターネットアクセスが可能になります。

データブローカーの設定を表示

データブローカーの詳細を確認することで、ホスト名、IP アドレス、使用可能な CPU や RAM など特定することができます。



BlueXPのコピーと同期には、データブローカーに関する次の詳細が表示されます。




- 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、データブローカーのバージョンなど
- ハードウェア：CPU と RAM
- 設定：データブローカーの 2 種類の主なプロセスの詳細（スキャナと転送元）



スキャナはソースとターゲットをスキャンし、コピーする対象を決定します。転送元は実際のコピーを行います。ネットアップの担当者は、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するための推奨アクションを提示することが

手順



1. [同期]>[データブローカーの管理]*を選択します。
2. 選択するオプション  をクリックして、グループ内のデータブローカーのリストを展開します。
3. 選択するオプション  をクリックしてください。


 tanyagcp0212  

2
Data Brokers

968.5 B/s
Transfer Rate




1
Relationships

 1 Active  1 Unknown
Data Brokers Status

 tanyagcp0212

GCP

Transfer Rate: 968.5 B/s

 Active  

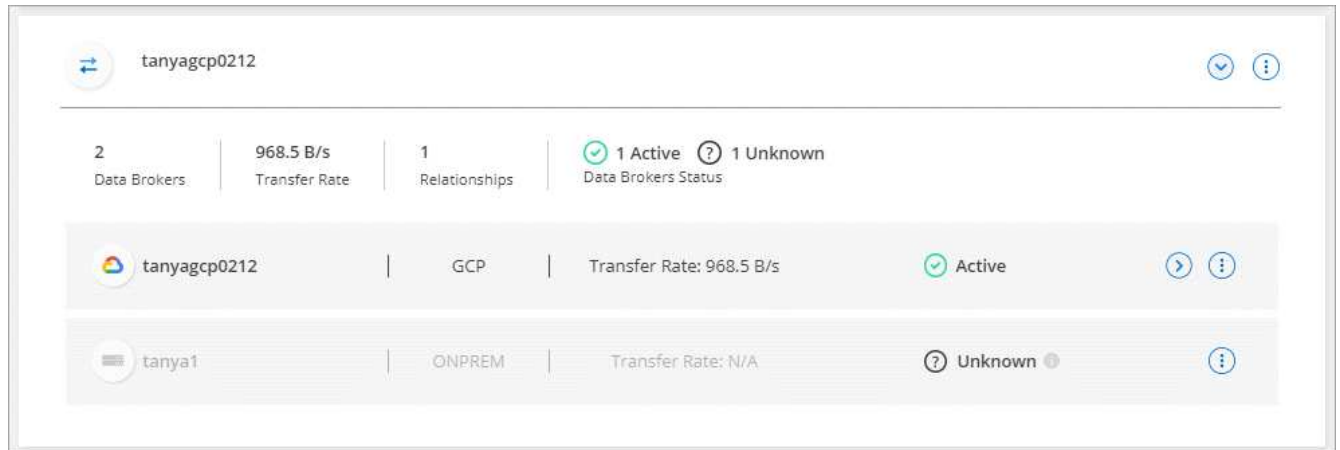
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project Id
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version
Hardware	4 Available CPUs	62.22 MB Available RAM		
Configuration	50 Scanner Concurrency	4 Scanner CPUs	50 Transferer Concurrency	4 Transferer CPUs


データブローカーの問題に対処

BlueXPのコピーと同期には、各データブローカーのステータスが表示され、問題のトラブルシューティングに役立ちます。

手順

1. ステータスが「Unknown」または「Failed」のデータブローカーを特定します。



2. の上にカーソルを置きます  アイコンをクリックして失敗の理由を確認してください。
3. 問題を修正します。

たとえば、オフラインのデータブローカーを再起動するだけで、初期導入に失敗した場合はデータブローカーの削除が必要になることがあります。


データブローカーをグループから削除

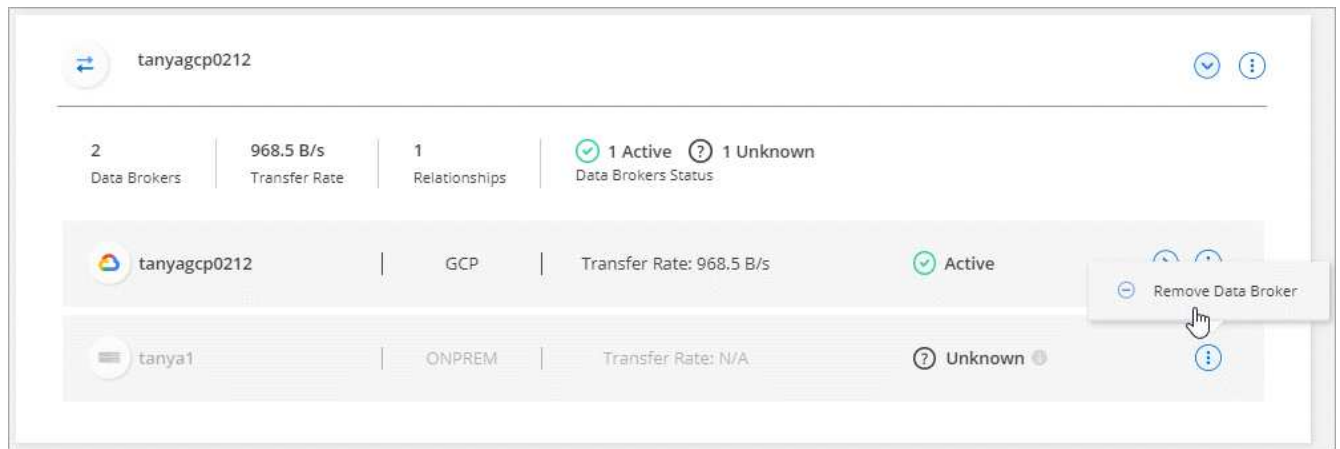
データブローカーが不要になった場合や初期導入に失敗した場合は、グループから削除することができます。この操作で削除されるのは、BlueXPのコピーと同期のレコードからのみです。データブローカーとその他のクラウドリソースについては、手動で削除する必要があります。

知っておくべきこと

- BlueXPのコピーと同期では、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。
- グループを使用している関係がある場合、その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. [同期]>[データブローカーの管理]*を選択します。
2. 選択するオプション  をクリックして、グループ内のデータブローカーのリストを展開します。
3. データブローカーの操作メニューを選択し、*[データブローカーの削除]*を選択します。



4. [データブローカーの削除]*を選択します。

結果

BlueXPの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。

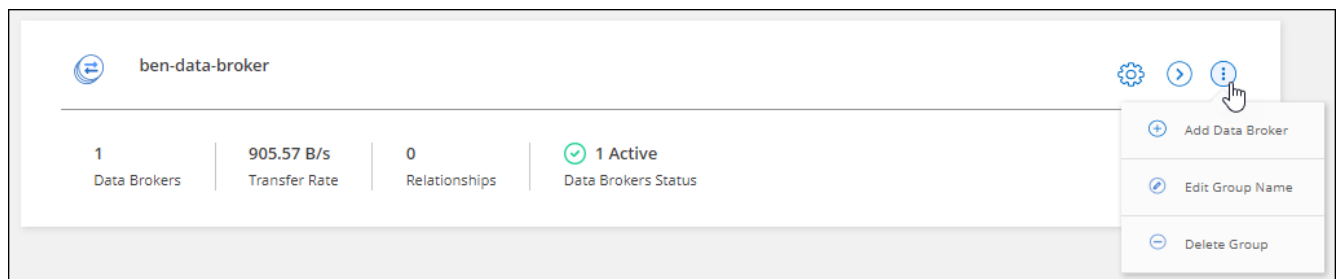
データブローカーグループを削除

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、BlueXPの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。

BlueXPのコピーと同期によって削除されたデータブローカーは、BlueXPのコピーと同期のレコードからのみ削除されます。クラウドプロバイダからデータブローカーインスタンスを手動で削除し、追加のクラウドリソースを削除する必要があります。

手順

1. [同期]>[データブローカーの管理]*を選択します。
2. 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。



3. 確認のために、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

BlueXPのコピーと同期によってデータブローカーが削除され、グループが削除されます。

レポートを作成および表示して、設定を調整します

レポートを作成して表示すると、ネットアップの担当者が支援する情報を入手して、データブローカーの設定を調整し、パフォーマンスを向上させることができます。

各レポートには、同期関係にあるパスに関する詳細情報が表示されます。たとえば、ファイルシステムのレポートには、ディレクトリとファイルの数、ファイルサイズの分布、ディレクトリの深さと幅などが表示されます。

レポートの作成

レポートを作成するたびに、BlueXPの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。

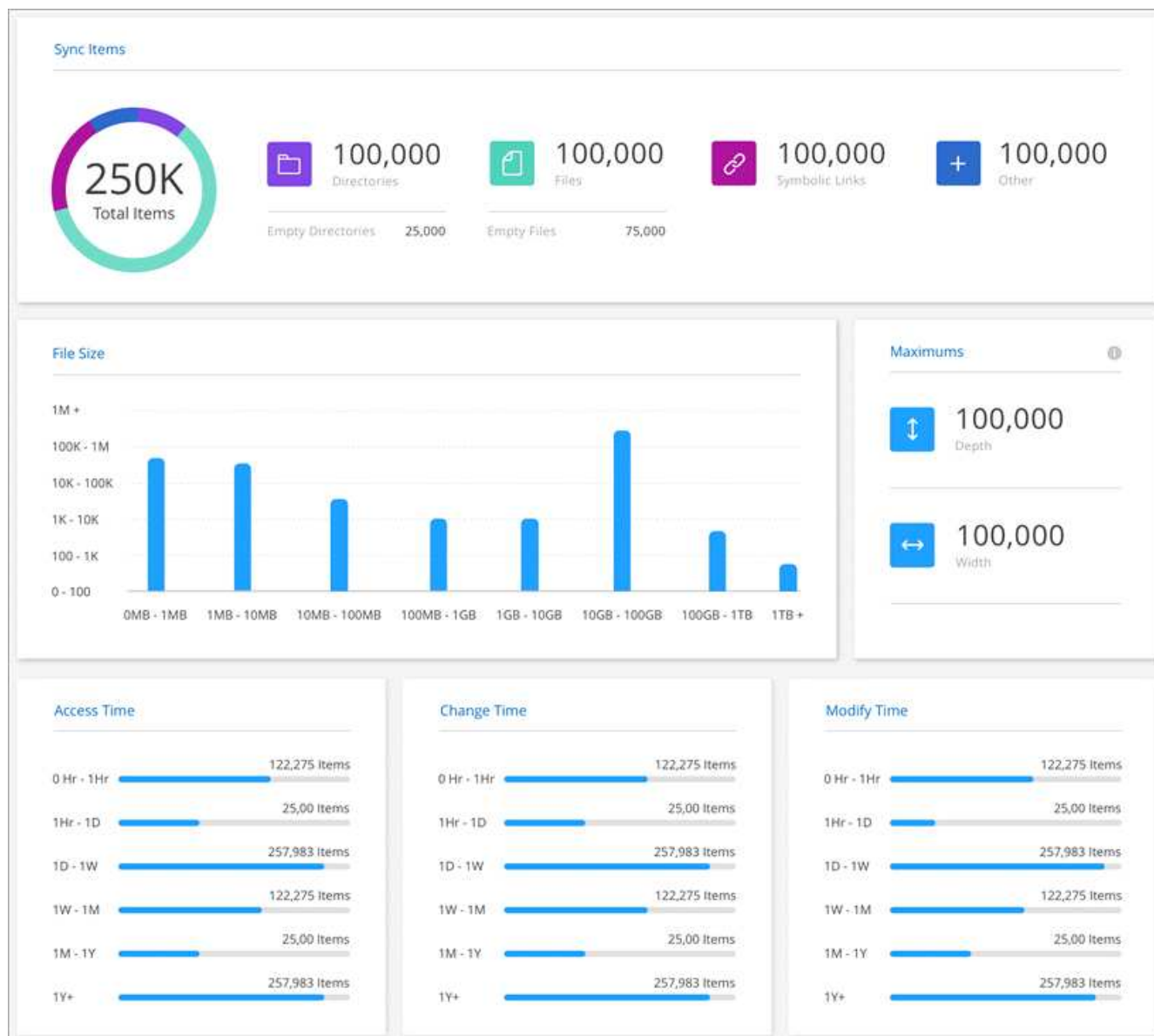
手順

1. [同期]>[レポート]*を選択します。

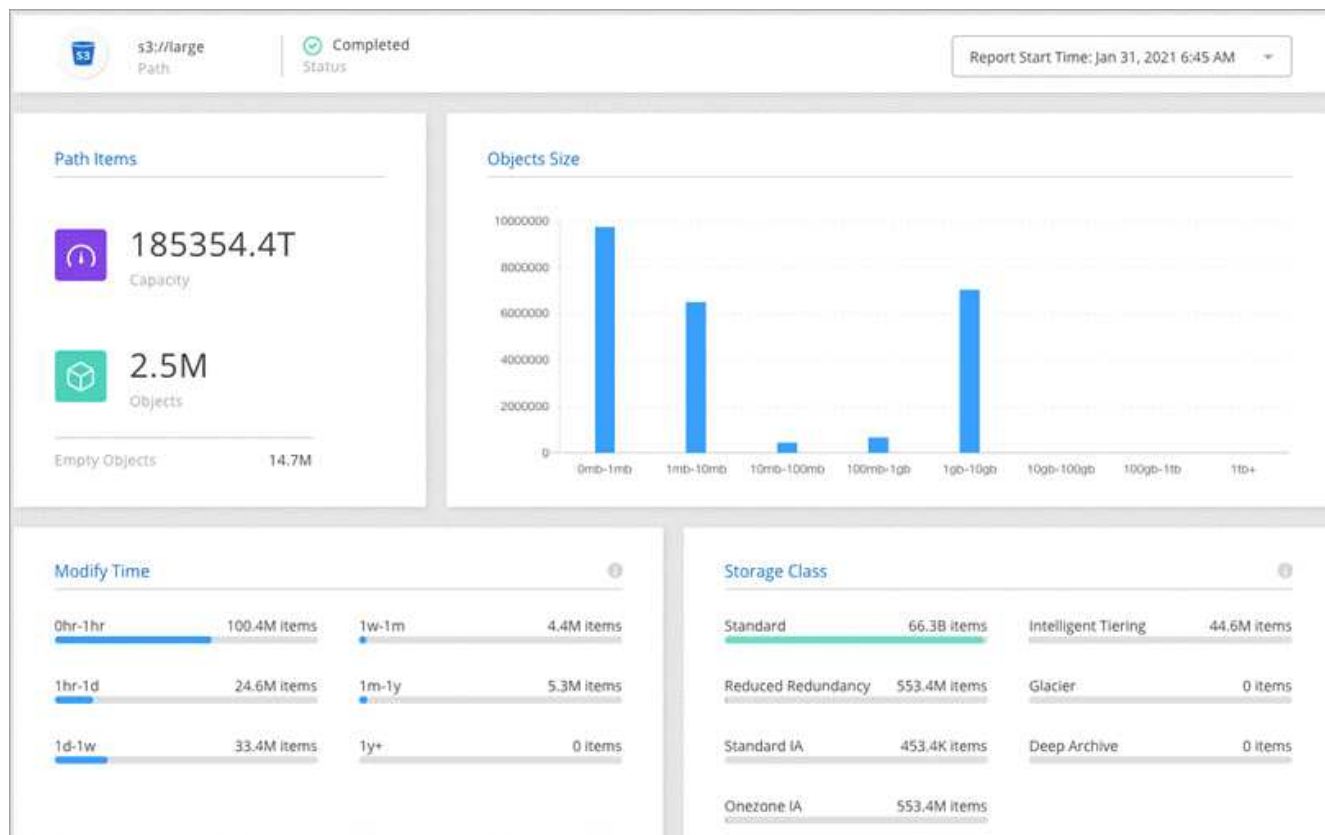
同期関係のそれぞれのパス（ソースまたはターゲット）が表形式で表示されます。

2. [レポートアクション（Reports Actions）]列で、特定のパスに移動して*を選択するか、アクションメニューを選択して[新規作成（Create New）]*を選択します。
3. 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て*表示*を選択します。

ファイルシステムパスのサンプルレポートを次に示します。



次に、オブジェクトストレージに関するレポートの例を示します。

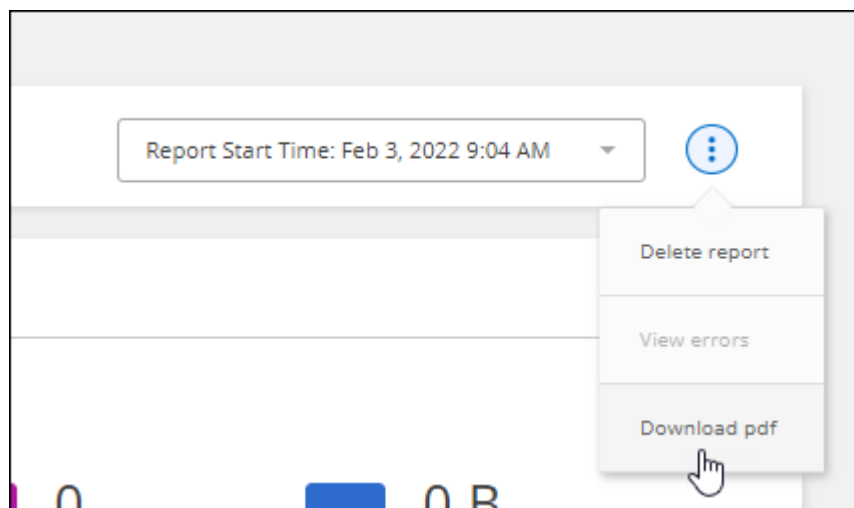


レポートのダウンロード

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できます。

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、アクションメニューを選択し、*[表示]*を選択します。
3. レポートの右上で、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。



オプションのスクリーンショット。"]

レポートエラーの表示

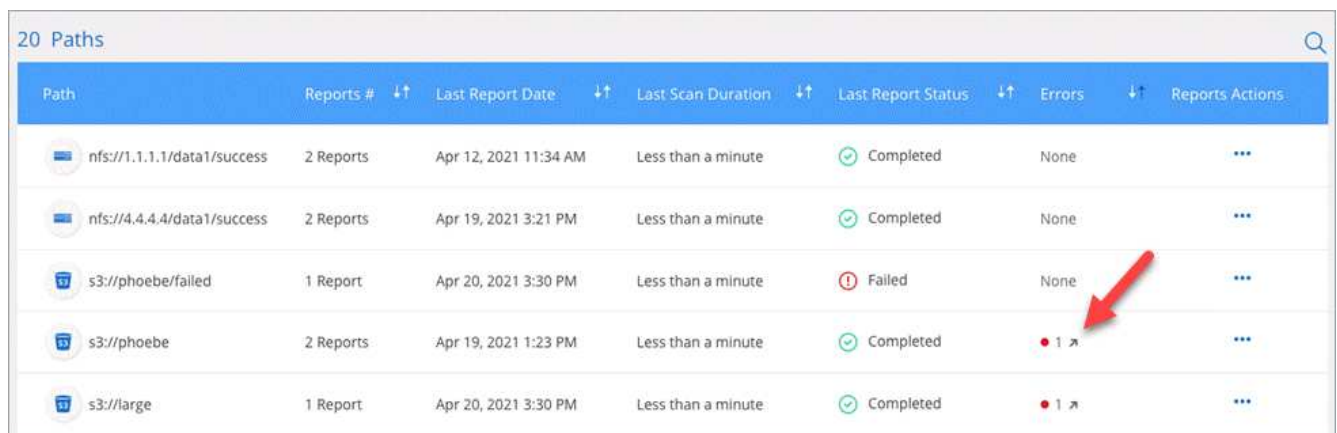
Paths テーブルは、最新のレポートにエラーがあるかどうかを示します。パスをスキャンしたときにBlueXPのコピーと同期が直面した問題 を示すエラーが表示されます。

たとえば、レポートに権限拒否エラーが含まれている場合があります。このエラーは、BlueXPのコピーと同期で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する可能性があります。

エラーのリストを確認したら、問題に対処してからレポートを再実行できます。

手順

1. [同期]>[レポート]*を選択します。
2. [エラー *] 列で、レポートにエラーがあるかどうかを確認します。
3. 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。



Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

テーブルのスクリーンショット。[Errors] 列にはクリック可能な小さな矢印が表示されています。"]

4. エラーの情報を使用して、問題を修正します。

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が表示されなくなります。

レポートの削除

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するレポートを削除することができます。

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。

データブローカーのアンインストール

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、およびデータブローカーのインストール時に作成されたパッケージと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（ /opt/NetApp/databroker' ）に変更します
3. 次のコマンドを実行します。

```
chmod +x アンインストーラ - databroker.sh` ./uninstaller - databroker.sh`
```

4. 「 y 」 を押してアンインストールを確定します。

BlueXPのコピーと同期のAPI

Web UIから利用できるBlueXPのコピーと同期の機能は、RESTful APIからも利用できます。

はじめに

BlueXPのコピーと同期APIの使用を開始するには、ユーザトークンとBlueXP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 BlueXPからユーザ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": "UaVhOIXMWQs5ilWdDxauXe5Mqkb34NJQ",
  "grant_type": "password",
  "password": "<user_password>"
}
```



クライアントIDのない個人用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「QC3AgHk6qdbmC7Yr82ApBwaaJLwRNO」を使用できます。

1. BlueXp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"
  }
]
```

2. 各 API 呼び出しの Authorization ヘッダーにユーザ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> は、前の手順で取得したトークンと ID で置き換えます。

```
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" }
```

トークンの有効期限が切れた場合はどうすればよいですか。

NetApp BlueXpのユーザ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 応答には、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。

API リファレンス

BlueXPのコピーと同期の各APIのドキュメントは、から入手できます <https://api.cloudsync.netapp.com/docs>。

List API の使用

list API は非同期 API であるため、結果はすぐには返されません (たとえば 'get/data-colders/{id}/list-nfs-export-folders' と 'get/data-colders/{id}/list-s3-bas' など) サーバからの応答は、HTTP ステータス 202 だけです。実際の結果を得るには 'get/mmessaging/client' API を使用する必要があります

手順

1. 使用するリスト API を呼び出します。
2. オペレーションの結果を表示するには 'get/mmessaging/client' API を使用します
3. 受信した ID を付加して、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 'get/mmessages/client' API を呼び出すたびに更新されることに注意してください

◦ 例 *

'list-s3-buckets' API を呼び出すと '結果はすぐには返されません

```
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>
```

その結果、HTTP ステータスコード 202 が生成されます。これは、メッセージが受け入れられたが、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持つ配列になります。ID フィールドは、サーバが最後に送信したメッセージを表します。例：

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

次に、受信した ID を使用して、次の API コールを実行します。

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です。各メッセージ内にはペイロードオブジェクトがあります。ペイロードオブジェクトは、動作の名前（キー）とその結果（値）で構成されます。例：

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


概念

ライセンスの概要

14 日間の無料トライアル終了後に、同期関係の料金を支払う方法は 2 通りあります。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払いのいずれかを購読することです。2 つ目の選択肢は、ネットアップから直接ライセンスを購入することです。

ライセンスの管理には、BlueXPのコピーと同期、または該当するWebサイトを使用する必要があります。デジタルウォレットを使用することはできません*。

Marketplace サブスクリプション

AWSまたはAzureからBlueXPのコピーおよび同期サービスにサブスクライブすると、時間単位または年単位で支払うことができます。"[AWS または Azure でサブスクライブできます](#)"、どこに課金するかによって異なります。

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 1 時間ごとに課金されます。

- ["Azure で価格を表示します"](#)
- ["AWS で従量課金制の価格を確認できます"](#)

年間サブスクリプション

年間サブスクリプションでは、事前に支払う 20 の同期関係のライセンスが提供されます。同期関係を 20 個以上に設定し、AWS から登録した場合は、追加の関係分を 1 時間単位で支払います。

["AWS の年間価格を確認します"](#)

ネットアップのライセンス

同期関係のコストを事前に支払うもう 1 つの方法は、ネットアップからライセンスを直接購入することです。各ライセンスでは、最大 20 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、25 の同期関係がある場合は、ライセンスを使用して最初の 20 の同期関係に料金を支払い、残りの 5 つの同期関係を持つ 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BlueXPのコピーと同期に追加する方法について説明します"](#)。

ライセンス条項

BlueXPのコピーおよび同期サービスでお客様所有のライセンスを使用（BYOL）する場合は、ライセンス使用権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 ライセンスを利用できます。
- お客様は、BYOL ライセンスを利用して、ソースとターゲットの間の合計 20 個の個別接続を確立することができます（それぞれ「同期関係」）。
- お客様の利用資格は、お客様が 20 件の同期関係の制限に達したかどうかに関係なく、1 年間のライセンス期間の終了時に期限切れとなります。
- 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から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は引き継がれません。

データのプライバシー

ネットアップでは、BlueXPのコピーと同期サービスの使用中に提供されたクレデンシャルには一切アクセスできません。クレデンシャルは、ネットワーク内の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、BlueXPのコピーと同期で、新しい関係の作成時にクレデンシャルの入力を求められることがあります。たとえば、SMB サーバを含む関係を設定する場合や、AWS にデータブローカーを導入する場合などです。

これらのクレデンシャルは、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、ネットワーク上のマシンに配置されます。クレデンシャルがネットアップに提供されることはありません。

クレデンシャルは、HanCorp Vault を使用してデータブローカーマシンでローカルに暗号化されます。

BlueXPのコピーと同期に関するテクニカルFAQ

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

はじめに

以下の質問は、BlueXPのコピーと同期の開始に関するものです。

BlueXPのコピーと同期の仕組み

BlueXPのコピーと同期は、ネットアップの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（これは_sync relationship_と呼ばれます）。

データブローカーグループは、ソースとターゲットの同期関係を制御します。同期関係を設定すると、BlueXPのコピーと同期によってソースシステムが分析され、複数のレプリケーションストリームに分割されて、選択したターゲットデータにプッシュされます。

最初のコピーの後、設定したスケジュールに基づいて変更されたデータが同期されます。

14 日間の無料トライアルはどのように機能しますか？

14日間の無償トライアルは、BlueXPのコピーと同期サービスに登録すると開始されます。14日間にわたって作成したBlueXPのコピーおよび同期関係については、ネットアップが料金を請求することはありません。ただし、導入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。

BlueXPのコピーと同期の料金はいくらですか？

BlueXPの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。

- サービス料金 *

従量課金制の場合、BlueXPのコピー/同期サービスは、作成する同期関係の数に基づいて時間単位で料金が発生します。

- ["AWS で従量課金制の価格を確認できます"](#)
- ["AWS の年間価格を確認します"](#)
- ["Azure で価格を表示します"](#)

BlueXPのコピーライセンスと同期ライセンスは、ネットアップの担当者からも入手できます。各ライセンスでは、12 カ月間で 20 の同期関係が有効になります。

["ライセンスの詳細については、こちらをご覧ください。"](#)



Cloud Volumes Service と Azure NetApp Files では、BlueXPのコピー関係と同期関係を無料で利用できます。

- 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。

BlueXPのコピーと同期の請求方法とサブスクリプションの管理方法を教えてください。

14 日間の無料トライアル終了後に、同期関係の料金を支払う方法は 2 通りあります。最初のオプションは、AWS または Azure から購読することです。AWS または Azure を使用すると、従量課金制または年払いが可能になります。2 つ目の選択肢は、ネットアップ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プロバイダのマーケットプレイスを通じて管理され、BlueXPのコピーと同期のユーザーインターフェイスでは*管理されません。

BlueXPのコピーと同期をクラウド外で使用できますか？

BlueXPのコピーと同期は、非クラウドアーキテクチャで使用できます。ソースとターゲットはオンプレミスに配置できるため、データブローカーソフトウェアを使用することもできます。

BlueXPのクラウド外でのコピーと同期の使用については、次の点に注意してください。

- データブローカーグループがBlueXPのコピーおよび同期サービスと通信するには、インターネット接続が必要です。
- ネットアップからライセンスを直接購入しない場合は、PAYGO BlueXPのコピーおよび同期サービスの請求にAWSまたはAzureのアカウントが必要になります。

BlueXPのコピーと同期へのアクセス方法を教えてください。

BlueXPのコピーと同期は、BlueXP Webサイトの*[Sync]*タブから実行できます。

データブローカーグループとは

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ています。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

同期関係でサポートされているソースとターゲットに関連する次の質問。

BlueXPのコピーと同期はどのソースとターゲットに対応していますか？

BlueXPのコピーと同期は、さまざまな種類の同期関係に対応しています。 ["リスト全体を表示します。"](#)。

BlueXPのコピーと同期では、NFSとSMBのどのバージョンがサポートされていますか？

BlueXPのコピーと同期では、NFSバージョン3以降とSMBバージョン1以降がサポートされます。

["同期の要件の詳細については、こちらをご覧ください。"](#)。

Amazon S3 がターゲットである場合、特定の S3 ストレージクラスにデータを階層化できますか。

はい。AWS S3 がターゲットである場合は、特定の S3 ストレージクラスを選択できます。

- 標準（これがデフォルトクラス）
- インテリジェント階層化
- 標準的なアクセス頻度は低い
- 1 回のアクセスではほとんど発生しません
- Glacier Deep Archive
- Glacierの柔軟な取得
- Glacier のインスタント検索

Azure BLOB ストレージのストレージ階層について教えてください。

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

- ホットストレージ
- 優れたストレージ

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。

- 標準
- ニアライン
- コールドライン（Coldline）
- Archive サービスの略

ネットワーキング

ここでは、BlueXPのコピーと同期のネットワーク要件について説明します。

BlueXPのコピーと同期のネットワーク要件を教えてください。

BlueXPのコピーおよび同期環境では、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）を使用してデータブローカーグループをソースとターゲットに接続する必要があります。

さらに、データブローカーグループがBlueXPのコピーおよび同期サービスと通信し、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経由のアウトバウンドインターネット接続が必要です。

詳細："[ネットワーク要件を確認します。](#)"。

データブローカーでプロキシサーバを使用できますか。

はい。

BlueXPのコピーと同期は、ベーシック認証の有無にかかわらずプロキシサーバに対応しています。データブローカーの導入時にプロキシサーバを指定した場合、データブローカーからの HTTP および HTTPS トラフィックはすべてプロキシ経由でルーティングされます。NFS や SMB などの HTTP 以外のトラフィックは、プロキシサーバ経由でルーティングできないことに注意してください。

プロキシサーバの唯一の制限は、NFS または Azure NetApp Files 同期関係で転送中のデータ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、プロキシサーバ経由でルーティングすることはできません。

データの同期

次の質問は、データ同期の仕組みに関連しています。

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、毎日の同期に設定されています。初期同期化の後、次の操作を実行できます。

- 同期スケジュールを、希望する日数、時間数、分数に変更します
- 同期スケジュールを無効にします
- 同期スケジュールを削除します（データは失われません。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？

データを 1 分ごとに同期するように関係をスケジュールできます。

データブローカーグループは、ファイルの同期に失敗したときに再試行しますか。またはタイムアウトしますか？

データブローカーグループは、1 つのファイルの転送が失敗しても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、同期関係の設定で設定できます。

"同期関係の設定を変更する方法について説明します。"。

非常に大規模なデータセットがある場合はどうすればよいですか。

1つのディレクトリに60万以上のファイルが含まれている場合は、データブローカーグループを設定してペイロードを処理できるように、mailto : ng-cloudsync-support@netapp.com [お問い合わせ]をご利用ください。データブローカーグループにメモリを追加しなければならない場合があります。

マウントポイント内のファイルの総数に制限はありません。上位ディレクトリやサブディレクトリの階層のレベルに関係なく、600、000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

セキュリティに関する次の質問

BlueXPのコピーと同期は安全ですか？

はい。BlueXPのコピーサービスと同期サービスのネットワーク接続は、すべてを使用して行います ["Amazon Simple Queue Service \(SQS\)"](#)。

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

BlueXPのコピーと同期をオンプレミス（ソースまたはデスティネーション）システムと使用する場合は、次の接続オプションを推奨します。

- AWS Direct Connect、Azure ExpressRoute、またはGoogle Cloud Interconnect 接続。インターネット経由ではない（指定したクラウドネットワークとのみ通信可能）
- オンプレミス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 クラウドストレージを使用した安全なデータ転送のために、Amazon Private S3 エンドポイント、Azure Virtual Network 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。

いずれの方法でも、オンプレミスのNASサーバとBlueXPのコピーおよび同期データブローカーグループの間にセキュアな接続を確立できます。

BlueXPのコピーと同期によってデータが暗号化されていますか？

- BlueXPのコピーと同期は、ソースとターゲットのNFSサーバ間の転送中データの暗号化に対応しています。"詳細はこちら"。
- SMBについては、BlueXPのコピーと同期でサーバ側で暗号化したSMB 3.0と3.11のデータがサポートされます。BlueXPのコピーと同期では、暗号化されたデータがソースからターゲットにコピーされ、ターゲットではデータが暗号化されたままになります。

BlueXPのコピーと同期では、SMBデータ自体は暗号化できません。

- Amazon S3バケットが同期関係のターゲットである場合は、AWS KMSの暗号化と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 Storageバケットが同期関係のターゲットである場合は、デフォルトのGoogle管理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、データ権限に関連しています。

SMB 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？

BlueXPのコピーと同期を設定して、ソースのSMB共有とターゲットのSMB共有の間、およびソースの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。



BlueXPのコピーと同期では、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 をコピーする方法について説明します。"。

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。

BlueXPのコピーと同期では、次のようにNFSサーバ間でNFS権限が自動的にコピーされます。

- NFSバージョン3：BlueXPのコピーと同期で権限とユーザグループの所有者がコピーされます。
- NFSバージョン4：BlueXPのACLのコピーと同期でコピー

オブジェクトストレージのメタデータ

BlueXPのコピーと同期では、次のタイプの同期関係のオブジェクトストレージメタデータがソースからターゲットにコピーされます。

- Amazon S3 → Amazon S3 ^1
- Amazon S3 → StorageGRID
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID の順にクリックします
- StorageGRID → Google Cloud Storage
- Google Cloud Storage → StorageGRID ^1
- Google Cloud Storage → IBM Cloud Object Storage ^1
- Google Cloud Storage → Amazon S3 ^1
- Amazon S3 → Google Cloud Storage
- IBM Cloud Object Storage → Google Cloud Storage
- StorageGRID → IBM クラウドオブジェクトストレージ
- IBM Cloud Object Storage → StorageGRID の順にクリックします
- IBM Cloud Object Storage → IBM Cloud Object Storage

^1 この同期関係には、以下が必要です "[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](#)"。

パフォーマンス

BlueXPのコピーと同期のパフォーマンスに関する質問を次に示します。

同期関係の進行状況インジケータは何を表していますか。

同期関係は、データブローカーグループのネットワークアダプタのスループットを示しています。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できますか。

大容量のファイル（それぞれ複数の TiB）がある場合は、転送プロセスが完了するまでに時間がかかることがあり、パフォーマンスに影響する可能性があります。

同時転送の数を制限すると効果的です。mailto : ng-cloudsync-support@netapp.com [お問い合わせ]

Azure NetApp Files でパフォーマンスが低いのはなぜですか？

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

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については、こちらをご覧ください](#)".

Cloud Volumes Service for AWS でパフォーマンスが低下するのはなぜですか。

クラウドボリュームとの間でデータを同期する場合、クラウドボリュームのパフォーマンスレベルが標準の場合は、障害やパフォーマンスの問題が発生することがあります。

サービスレベルを Premium または Extreme に変更して、同期のパフォーマンスを向上させます。

1 つのグループに必要なデータブローカーの数

新しい関係を作成する場合は、1 つのデータブローカーを 1 つのグループで開始します（アクセラレーション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、1 つ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。同期されていない場合は、データブローカーをグループに追加することで、同期パフォーマンスを高速化できます。ただし、まず、同期の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、複数の要因が影響します。全体的な同期パフォーマンスは、ネットワーク帯域幅、レイテンシ、ネットワークトポロジ、データブローカー VM の仕様、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が 100MB/s に達することはありますが、ターゲットのディスクスループットでは 64MB/s しか許可されません。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、ターゲットではデータブローカーグループのパフォーマンスを達成できません。

そのため、ネットワークのパフォーマンスとターゲットのディスクスループットを確認してください。

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共有することで、同期パフォーマンスを高速化することを検討します。 "[同期のパフォーマンスを高速化する方法について説明します](#)".

項目を削除する

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連しています。

BlueXPのコピーと同期関係を削除するとどうなりますか？

関係を削除すると、以降のすべてのデータの同期が停止し、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ていますか？

デフォルトでは、Active Sync 関係がある場合、ソースサーバ上で削除されたアイテムは、次の同期時にターゲットから削除されません。ただし、関係ごとの同期設定にはオプションがあり、BlueXPのコピーと同期でターゲットの場所にあるファイルがソースから削除された場合に削除されるように定義できます。

["同期関係の設定を変更する方法について説明します。"](#)

ターゲットから何かを削除するとどうなりますか？ソースからも削除されていますか？

ターゲットから削除されたアイテムは、ソースから削除されません。ソースからターゲットへの関係は一方向です。次の同期サイクルでは、BlueXPのコピーと同期によってソースとターゲットが比較され、アイテムが見つからないことが特定され、BlueXPのコピーと同期によってソースからターゲットにもう一度コピーされます。

トラブルシューティング

["ネットアップナレッジベース：BlueXP copy and sync FAQ：Support and Troubleshooting"](#)

データブローカーのディープダイブ

次の質問は、データブローカーに関連しています。

データブローカーのアーキテクチャについて説明できますか？

確かに。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ている Node.js アプリケーションです。
- BlueXPのコピーと同期は、次のようにデータブローカーを導入します。
 - AWS : AWS Cloudformation テンプレートから
 - Azure : Azure Resource Manager 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します。
- データブローカーは、AWS SQS を信頼性の高い安全な通信チャネルとして使用し、制御と監視を行います。SQS は永続性レイヤも提供します。
- データブローカーをグループに追加することで、転送速度を向上させ、高可用性を追加することができます。1つのデータブローカーに障害が発生した場合、サービスの耐障害性があります

知識とサポート

サポートに登録します

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、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のファイルサービスでNetAppのサポートは有効になりません。クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- ["ONTAP 対応の Amazon FSX"](#)
- ["Azure NetApp Files の特長"](#)
- ["Cloud Volumes Service for Google Cloud"](#)

サポート登録の概要

サポート資格を有効にする登録には、次の2つの形式があります。

- BlueXPアカウントIDサポートサブスクリプションの登録(BlueXP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)。

これは、BlueXP内のすべてのサービスのシングルサポートサブスクリプションIDとして機能します。各BlueXPアカウントレベルのサポート契約が登録されている必要があります。

- クラウドプロバイダのマーケットプレイスでのサブスクリプションに関連付けられているCloud Volumes ONTAP のシリアル番号を登録している (909201xxxxxxxxのシリアル番号)。

これらのシリアル番号は、通常PAY_GOシリアル番号と呼ばれ、Cloud Volumes ONTAP の導入時にBlueXP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ことで、サポートチケットのオープンやケースの自動生成などの機能を利用できます。登録を完了するには、以下の手順でNetApp Support Site (NSS) アカウントをBlueXPに追加してください。

NetAppサポートにBlueXPアカウントに登録します

サポートに登録してサポート利用資格をアクティブ化するには、BlueXPアカウントの1人のユーザがNetApp Support SiteアカウントをBlueXPログインに関連付ける必要があります。ネットアップサポートへの登録方法は、NetApp Support Site (NSS) アカウントがある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のお客様

NSSアカウントをお持ちのネットアップのお客様は、BlueXPからサポートに登録するだけで済みます。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[クレデンシャル]*を選択します。

2. [ユーザクレデンシャル]*を選択します。
3. [NSSクレデンシャルの追加]*を選択し、NetApp Support Site (NSS) 認証プロンプトに従います。
4. 登録プロセスが正常に完了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、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BlueXPユーザにNetApp Support Siteアカウントが関連付けられていない場合、このサポート登録ステータスは表示されません。ただし、BlueXPアカウントがサポートに登録されていないわけではありません。アカウント内の1人のユーザがこれらの手順を実行している限り、アカウントは登録されています。

NSSアカウントを持たない既存のお客様

NetAppの既存のお客様で、ライセンスとシリアル番号は_NO_NSSアカウントしかお持ちでない場合は、NSSアカウントを作成してBlueXPログインに関連付ける必要があります。

手順

1. を実行してNetApp Support Site アカウントを作成します ["NetApp Support Site ユーザー登録フォーム"](#)
 - a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
 - b. 必ず、上記のシリアル番号フィールドに使用されているBlueXPアカウントのシリアル番号(960xxxx)を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. の手順を実行して、新しいNSSアカウントをBlueXPログインに関連付けます [NSSアカウントをお持ちの既存のお客様](#)。

ネットアップのソリューションを初めて導入する場合は

ネットアップ製品を初めてご利用になり、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

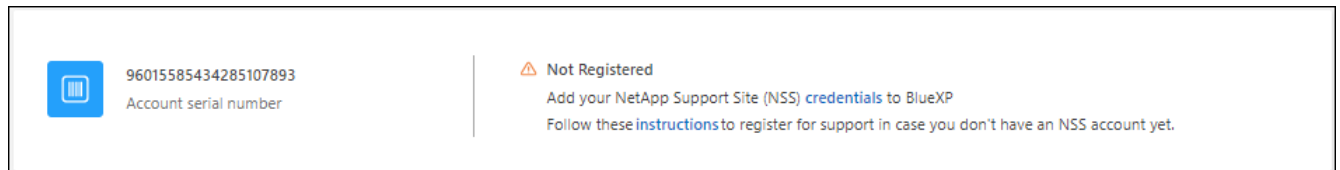
1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット

ト。サポートは最初に表示されるオプションです"]

2. サポート登録ページでアカウントIDのシリアル番号を確認します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. に移動します "ネットアップサポート登録サイト" 「ネットアップ登録のお客様ではありません」を選択します。
4. 必須フィールドに入力します（赤いアスタリスクのフィールド）。
5. [製品ライン（Product Line）]フィールドで、[Cloud Manager *]を選択し、該当する課金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、ネットアップのグローバルデータプライバシーポリシーを確認します。

この安全なトランザクションを完了するために、メールボックスに電子メールがすぐに送信されます。確認メールが数分で届かない場合は、必ずスパムフォルダを確認してください。

7. Eメールからアクションを確認します。

確認ではネットアップにリクエストが送信され、NetApp Support Site アカウントを作成することを推奨します。

8. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
 - a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
 - b. シリアル番号フィールドには、上記のアカウントのシリアル番号（960xxxx）を必ず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。

完了後

このプロセスについては、ネットアップからご連絡ください。これは、新規ユーザ向けの1回限りのオンボーディング演習です。

NetApp Support Siteアカウントを作成したら、の順序を実行してアカウントをBlueXPログインに関連付けます [NSSアカウントをお持ちの既存のお客様](#)。

Cloud Volumes ONTAPサポートのためにNSSクレデンシャルに関連付けます

NetApp Support Siteで次の主要なワークフローを有効にするには、BlueXPアカウントにクレデンシャルに関連付ける必要がCloud Volumes ONTAPあります。

- 従量課金制のCloud Volumes ONTAPシステムのサポートを登録しています

お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、NSS アカウントを用意する必要があります。

- お客様所有のライセンスを使用（BYOL）する場合のCloud Volumes ONTAP の導入

ライセンスキーをBlueXPでアップロードし、購入した契約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、期間の更新の自動更新も含まれます。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードしています

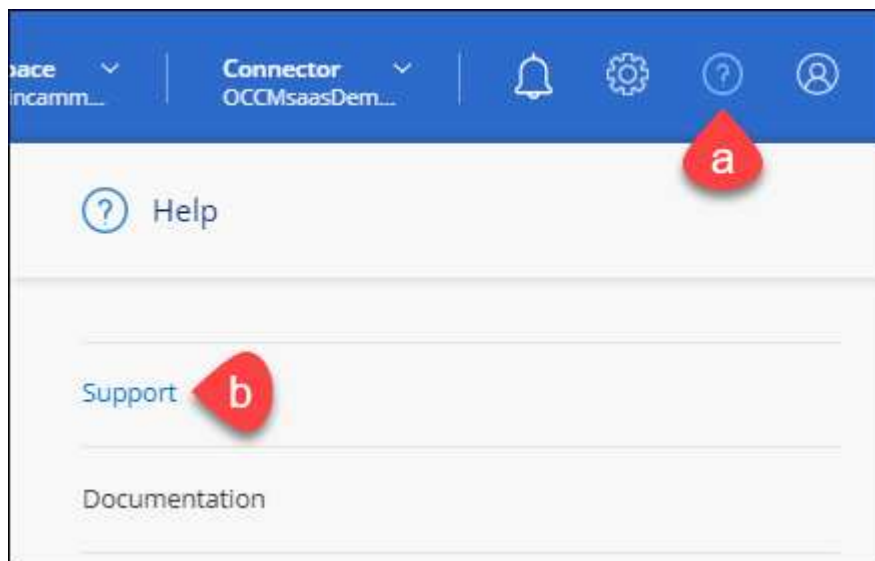
NSSクレデンシャルをBlueXPアカウントに関連付ける方法は、BlueXPユーザログインに関連付けられたNSSアカウントとは異なります。

これらのNSSクレデンシャルは、特定のBlueXPアカウントIDに関連付けられています。BlueXPアカウントに属するユーザは、*[サポート]>[NSS管理]*からこれらのクレデンシャルにアクセスできます。

- お客様レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することもできます。
- パートナーアカウントまたはリセラーアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することはできますが、お客様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. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [NSS Management]>[Add NSS Account]*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では、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

4. ログインページで、ネットアップサポートサイトの登録 E 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、BlueXPはライセンスのダウンロード、ソフトウェアのアップグレード検証、および将来のサポート登録などの目的でNSSアカウントを使用できます。

次の点に注意してください。

- NSSアカウントは、お客様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）。複数のお客様レベルのNSSアカウントを設定できます。
- NSSアカウントがパートナーレベルのアカウントの場合、作成できるNSSアカウントは1つだけです。お客様レベルのNSSアカウントを追加しようとすると、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。

「別のタイプの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ていません。」

既存のお客様レベルの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。

- ログインに成功すると、ネットアップはNSSのユーザ名を保存します。

これはシステムによって生成されたIDで、電子メールにマッピングされます。[**NSS Management**]ページで、から電子メールを表示できます [...](#) メニュー。

- ログイン認証情報トークンを更新する必要がある場合は、の[認証情報の更新*]オプションも使用できます [...](#) 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に求められます。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ります。このことを通知する通知が投稿されます。

ヘルプを表示します

ネットアップでは、BlueXPとそのクラウドサービスをさまざまな方法でサポートしています。ナレッジベース（KB）記事やコミュニティフォーラムなど、24時間365日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

クラウドプロバイダのファイルサービスのサポート

クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- ["ONTAP 対応の Amazon FSX"](#)
- ["Azure NetApp Files の特長"](#)
- ["Cloud Volumes Service for Google Cloud"](#)

BlueXPおよびそのストレージソリューションとサービスに固有のテクニカルサポートを受けるには、以下に記載されてい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します

次のオプションは、1日24時間、週7日間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のマニュアル。

- ["ナレッジベース"](#)

BlueXPナレッジベースで問題のトラブルシューティングに役立つ記事を検索します。

- ["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できます。

ネットアップサポートと一緒にケースを作成します

上記のセルフサポートオプションに加え、サポートを有効にしたあとで問題が発生した場合は、ネットアップサポートの担当者と相談して解決できます。

始める前に

- [ケースの作成]*機能を使用するには、最初にNetApp Support Siteクレデンシャルを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ているクレデンシャルの管理方法について説明します"](#)。
- シリアル番号のあるONTAPシステムのケースをオープンする場合は、そのシステムのシリアル番号にNSSアカウントを関連付ける必要があります。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. **[Resources]**ページで、**[Technical Support]**で次のいずれかのオプションを選択します。
 - a. 電話で誰かと話をしたい場合は、*[電話]*を選択します。netapp.comのページに移動し、電話番号が表示されます。
 - b. [ケースの作成]*を選択して、NetAppサポートスペシャリストとのチケットをオープンします。
 - **Service:**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を備えたテクニカルサポート問題 に固有のBlueXPなどです。
 - **作業環境:**ストレージに該当する場合は、* Cloud Volumes ONTAP *または*オンプレミス*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、サービスの上部バナーで選択したBlueXPアカウント、ワークスペース、コネクタの範囲内にあります。

- ケース優先度：ケースの優先度を選択します。優先度は、[低]、[中]、[高]、[クリティカル]のいずれかになります。

これらの優先度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ポインタを合わせます。

- *事象の説明*：実行したエラーメッセージやトラブルシューティング手順など、問題の詳細な概要を入力します。
- その他のメールアドレス：この問題を他のユーザーに知らせる場合は、追加のメールアドレスを入力します。
- 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できます。

添付ファイルはファイルあたり25 MBに制限されています。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、およびcsv。

ntapitdemo 


NetApp Support Site Account

Service

Select ▼

Working Enviroment


Select ▼

Case Priority 

Low - General guidance ▼

Issue Description



Provide detailed description of problem, applicable error messages and troubleshooting steps taken.



Additional Email Addresses (Optional) 

Type here

Attachment (Optional)

No files selected

 Upload 

完了後

ポップアップにサポートケース番号が表示されます。ネットアップのサポート担当者がケースを確認し、すぐに対応させていただきます。

サポートケースの履歴を確認するには、*[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検索します。右端のボタンをクリックすると、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の会社が、BlueXPアカウントのシリアル番号(例960xxxx) または動作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、サポートを受けることができます。

- 製品内のチャットを使用します
- テクニカル以外のケースをに送信します <https://mysupport.netapp.com/site/help>

サポートケースの管理（プレビュー）

アクティブなサポートケースと解決済みのサポートケースは、BlueXPから直接表示および管理できます。NSSアカウントと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使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

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NSSアカウントによって過去3カ月間にオープンされたケースの総数が表示されます。
 - 右側のビューには、ユーザのNSSアカウントに基づいて、過去3カ月間にオープンしたケースの総数が会社レベルで表示されます。

テーブルの結果には、選択したビューに関連するケースが反映されます。

- 目的の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。他の列には、並べ替え機能だけがあります。

詳細については、以下の手順を参照してください。

- ケースごとに、ケースノートを更新したり、ステータスが「Closed」または「Pending Closed」でないケースをクローズしたりすることができます。

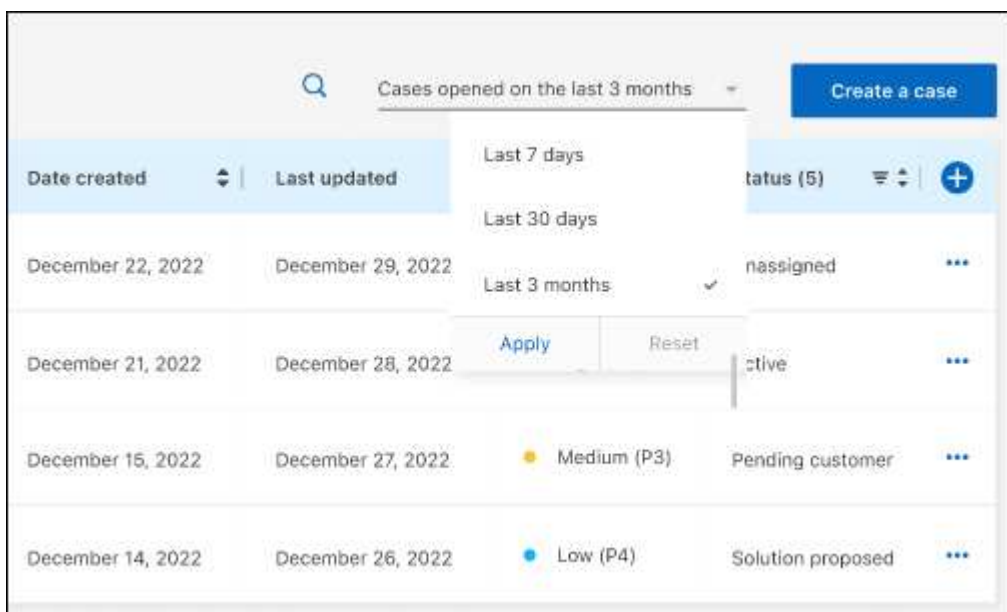
手順

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ユーザアカウントに関連付けられた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。

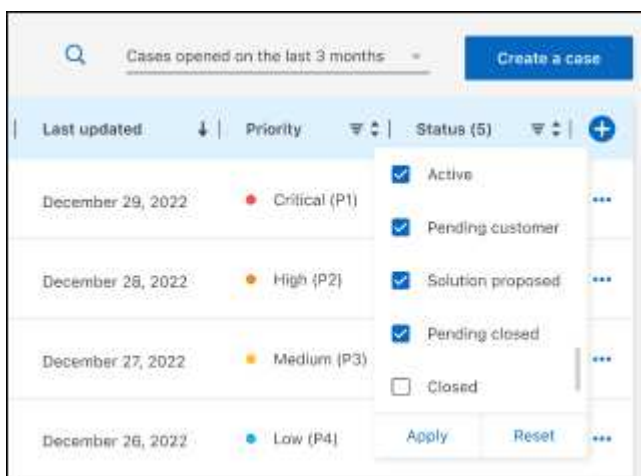
3. 必要に応じて、テーブルに表示される情報を変更します。

- [Organization's Cases]*で[View]*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。




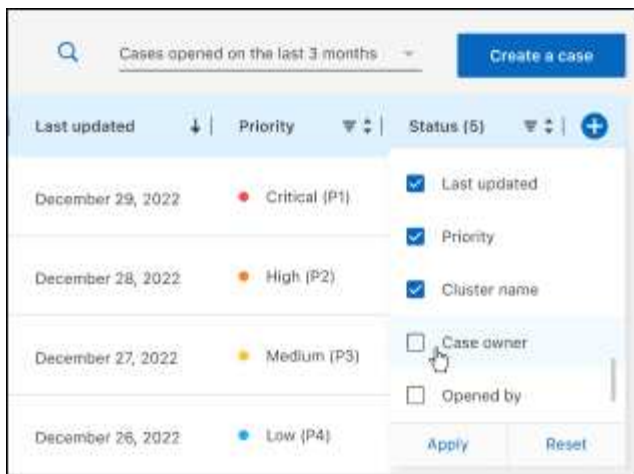
ページのテーブルの上にあるオプションのスクリーンショット。正確な日付範囲、または過去7日、30日、または3カ月を選択できます。"]

- 列の内容をフィルタリングします。



列のフィルタオプションのスクリーンショット。[Active]や[Closed]など、特定のステータスに一致するケースを除外できます。"]

- テーブル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。

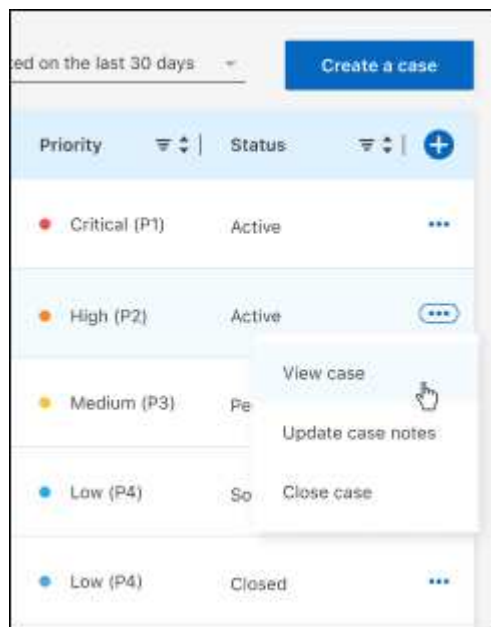


4. 既存のケースを管理するには、... 使用可能なオプションのいずれかを選択します。

- ケースの表示: 特定のケースの詳細を表示します。
- ケースノートの更新: 問題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あたり25 MBに制限されています。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、およびcsv。

- ケースをクローズ: ケースをクローズする理由の詳細を入力し、*ケースをクローズ*を選択します。



法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<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/"](https://www.netapp.com/company/legal/privacy-policy/)

オープンソース

通知ファイルには、ネットアップ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記載されています。

["BlueXPのコピーと同期に関するお知らせです"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記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。