Data Transfer Hub

実装ガイド

2022 年 1 月

目次

はじめに 4
コスト 5
Amazon S3 転送タスクのコスト 6
Amazon ECR 転送タスクのコスト 8
アーキテクチャの概要 9
ソリューションコンポーネント 14
セキュリティ 15
IAM ロール 15
Amazon CloudFront 16
設計に関する考慮事項 16
デプロイ可能なリージョン 16
AWS CloudFormation テンプレート 18
自動デプロイ 18
デプロイの概要 18
ステップ 1. (オプション 1) AWS リージョンでのスタックの起動 19
ステップ 1. (オプション 2) AWS 中国リージョンでスタックを起動する 21
ステップ 2. ウェブコンソールを起動する 25
ステップ 3. 転送タスクを作成する 26
その他のリソース 30

ソリューションのアンインストール.....30
AWS マネジメントコンソールの使用 30
AWS Command Line Interface の使用 31
Amazon S3 バケットの削除 31
ソースコード 32
ドキュメントの改訂.....32
寄稿者.....32
注意.....33

はじめに

「Data Transfer Hub」ソリューションは、Amazon Simple Storage Service (Amazon S3) のオブジェクトと Amazon Elastic Container Registry (Amazon ECR) のイメージのために、安全かつスケーラブルで追跡可能なデータ転送を提供します。このデータ転送は、AWS 中国リージョンとの間でビジネスをグローバルに拡大するのに役立ちます。

このソリューションのウェブコンソールには、次のタスクを管理するためのインターフェイスが用意されています。

- AWS 中国リージョンと AWS リージョンの間で Amazon S3 のオブジェクトを転送する
- 他のクラウドプロバイダーのオブジェクトストレージサービス (Alibaba Cloud OSS、Tencent COS、Qiniu Kodo など) から Amazon S3 にデータを転送する
- Amazon S3 互換オブジェクトストレージサービスから Amazon S3 にオブジェクトを転送する
- AWS 中国リージョンと AWS リージョンの間で Amazon ECR のイメージを転送する
- パブリックコンテナレジストリ (Docker Hub、Google gcr.io、Red Hat Quay.io など) から Amazon ECR にコンテナイメージを転送する

> **注意**: AWS リージョン間で Amazon S3 のオブジェクトを転送する必要がある場合は、クロスリージョンレプリケーションを使用することをお勧めします。同じ AWS リージョン内で Amazon S3 のオブジェクトを転送する場合は、同一リージョンレプリケーションを使用することをお勧めします。

この実装ガイドでは、アマゾン ウェブ サービス (AWS) クラウドに「Data Transfer Hub」ソリューションをデプロイするためのアーキテクチャ上の考慮事項と設定手順について説明します。このガイドには、AWS CloudFormation テンプレートへのリンクが含まれています。このテンプレートを使用すると、セキュリティと可用性に関する AWS のベストプラクティスに準拠してソリューションをデプロイするために必要な AWS のサービスを起動および設定できます。

このガイドは、AWS クラウドにおけるアーキテクチャ設計の実務経験を持つ IT アーキテクト、デベロッパー、DevOps スタッフ、データアナリスト、マーケティング技術のプロフェッショナルを対象としています。

コスト

このソリューションの実行中に使用した AWS サービスのコストは、お客様の負担となります。コストは Amazon S3 のオブジェクトと Amazon ECR のイメージのどちらを転送するかによって異なります。

このソリューションでは、静的なウェブサイトアセットを AWS アカウントに保存するための追加の Amazon CloudFront ディストリビューションと Amazon S3 バケットを自動的にデプロイします。これらのサービスから発生する変動料金は、お客様の負担になります。詳細については、このソリューションで使用する AWS の各サービスの料金表ウェブページを参照してください。

次に、コストの見積もりの例を示します。最初の 2 つは Amazon S3 のオブジェクトを転送する場合の見積もり例で、残りの 1 つは Amazon ECR のイメージを転送する場合の例です。

Amazon S3 転送タスクのコスト

Amazon S3 転送タスクの場合、コストはファイルの合計数と平均ファイルサイズによって異なります。

例 1: 2022 年 1 月時点で、AWS オレゴンリージョン (us-west-2) から AWS 北京リージョン (cn-north-1) に 1 TB の S3 ファイルを転送。平均ファイルサイズは **50 MB**。

- 合計ファイル数: 最大 2,048
- Amazon EC2 インスタンスあたりの平均速度: 最大 1 GB/分
- Amazon EC2 インスタンスの合計時間: 最大 17 時間

AWS のサービス	ディメンション	合計コスト
Amazon EC2	1 時間あたり 0.0084 USD (t4g.micro)	0.14 USD
Amazon S3	1 ファイルあたり最大 12 GET リクエスト + 10 PUT リクエスト GET: 1,000 リクエストあたり 0.0004 USD PUT: 1,000 リクエストあたり 0.005 USD	0.11 USD
Amazon DynamoDB	1 ファイルあたり最大 2 件の書き込みリクエスト 100 万書き込みあたり 1.25 USD	0.01 USD
Amazon SQS	1 ファイルあたり最大 2 件のリクエスト 100 万リクエストあたり 0.40 USD	0.01 USD
データ転送 (送信)	1 GB あたり 0.09	92.16 USD
その他 (Amazon CloudWatch、AWS Secrets Manager など)		最大 1 USD
	合計:	最大 93.43 USD

例 2: 2022 年 1 月時点で、AWS オレゴンリージョン (us-west-2) から中国本土北京リージョン (cn-north-1) に 1 TB の S3 ファイルを転送。平均ファイルサイズは **10 KB**。

- 合計ファイル数: 最大 107,400,000
- Amazon EC2 インスタンスあたりの平均速度: 最大 6 MB/分 (1 秒あたり最大 10 ファイル)
- Amazon EC2 インスタンスの合計時間: 最大 3,000 時間

AWS のサービス	ディメンション	合計コスト
Amazon EC2	1 時間あたり 0.0084 USD (t4g.micro)	25.20 USD
Amazon S3	1 ファイルあたり最大 2 GET リクエスト + 1 PUT リクエスト GET: 1,000 リクエストあたり 0.0004 USD PUT: 1,000 リクエストあたり 0.005 USD	622.34 USD
Amazon DynamoDB	1 ファイルあたり最大 2 件の書き込みリクエスト 100 万書き込みあたり 1.25 USD	268.25 USD
Amazon SQS	1 ファイルあたり最大 2 件のリクエスト 100 万リクエストあたり 0.40 USD	85.92 USD
データ転送 (送信)	1 GB あたり 0.09	92.16 USD
その他 (Amazon CloudWatch、Secrets Manager など)		20 USD
	合計:	最大 1113.87 USD

Amazon ECR 転送タスクのコスト

Amazon ECR 転送タスクの場合、コストはネットワーク速度と Amazon ECR イメージの合計サイズによって異なります。

例 3: 2022 年 1 月時点で、AWS アイルランドリージョン (eu-west-1) から AWS 北京リージョン (cn-north-1) に 27 の Amazon ECR イメージ (合計サイズ最大 3 GB) を転送。合計ランタイムは約 6 分。

AWS のサービス	ディメンション	合計コスト
AWS Lambda	100 ミリ秒あたり 0.0000004 USD	0.000072 USD (35221.95 ミリ秒)
AWS Step Functions	1 状態遷移あたり 0.000025 USD (ここでは実行ごとに最大 60 の状態遷移)	0.0015 USD
AWS Fargate	1 時間あたりの 1 vCPU 利用につき 0.04048 USD 1 時間あたりの 1 GB 利用につき 0.004445 USD (0.5 vCPU 1 GB メモリ)	0.015 USD (最大 2,200 秒)
データ転送 (送信)	1 GB あたり 0.09	0.27 USD
その他 (Amazon CloudWatch、AWS Secrets Manager など)	コストはほぼゼロ	0 USD
	合計:	最大 0.287 USD

アーキテクチャの概要

「Data Transfer Hub」ソリューションをデフォルトのパラメータでデプロイすると、AWS クラウドに次の環境が構築されます。

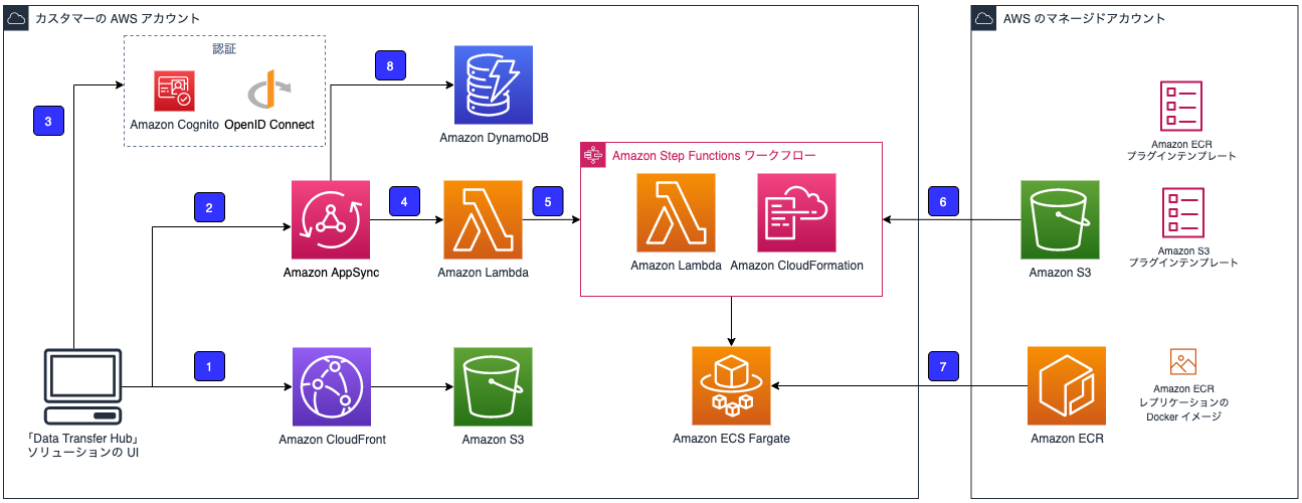

図 *1:* 「*Data Transfer Hub*」ソリューションのアーキテクチャ

このソリューションは、次のサービスを使用してサーバーレスアーキテクチャを自動的にデプロイおよび設定します。

1. ソリューションの静的ウェブアセット（フロントエンドユーザーインターフェイス）は、Amazon S3 に保存され、Amazon CloudFront を介して利用できます。

2. バックエンド API は、AWS AppSync GraphQL を介して提供されます。

3. ユーザーは、Amazon Cognito ユーザープール (AWS リージョンの場合) または OpenID 接続プロバイダー (AWS 中国リージョンの場合) (Authing、Auth0 など) によって認証されます。

4. AWS AppSync は、AWS Lambda を実行してバックエンド API を呼び出します。

5. AWS Lambda は、AWS CloudFormation を使用して Amazon ECR または Amazon S3 プラグインテンプレートを開始または停止/削除する AWS Step Functions ワークフローを開始します。

6. プラグインテンプレートは、AWS が管理する一元化された Amazon S3 バケットでホストされます。

7. このソリューションは、プラグインテンプレートで使用されるコンテナイメージを実行する Amazon ECS クラスターもプロビジョニングし、そのコンテナイメージは Amazon ECR でホストされます。

8. データ転送タスクに関する情報は Amazon DynamoDB に保存されます。

> **重要:** このソリューションを、Beijina Sinnet Technology Co., Ltd. (Sinnet) が運営する AWS (北京) リージョン、または Ningxia Western Cloud Data Technology Co., Ltd. が運営する AWS (寧夏) リージョンでデプロイする場合、ウェブコンソールにアクセスする前に、ドメインに ICP Recordal を提供する必要があります。

ウェブコンソールでは、すべてのデータ転送ジョブを一元的に作成および管理できます。各データタイプ (例えば、Amazon S3 または Amazon ECR) は、「Data Transfer Hub」ソリューションのプラグインであり、AWS が所有する Amazon S3 バケットでホストされる AWS CloudFormation テンプレートとしてパッケージ化されます。転送タスクを作成すると、AWS Lambda 関数が Amazon CloudFormation テンプレートを開始し、各タスクの状態が Amazon DynamoDB テーブルに保存および表示されます。

このソリューションは、2 つのデータ転送プラグイン (Amazon S3 プラグインと Amazon ECR プラグイン) をサポートしています。

Amazon S3 プラグイン

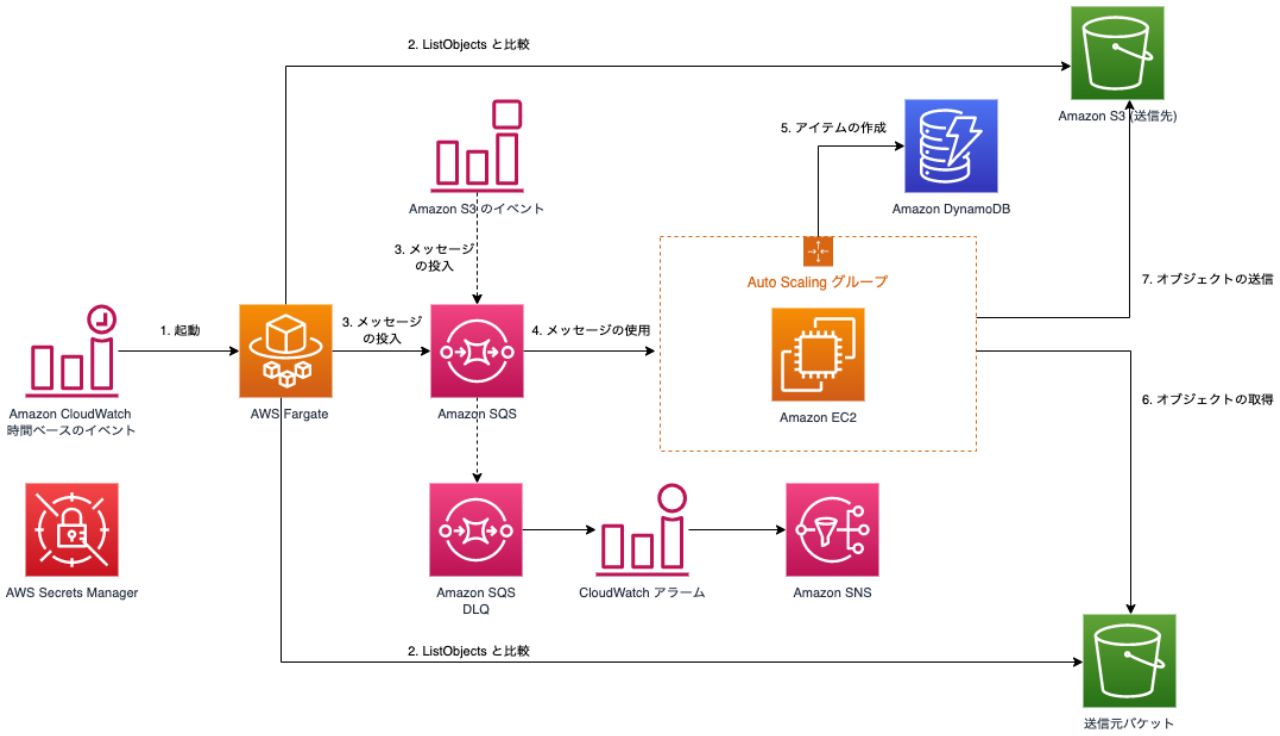

図 *2:*「*Data Transfer Hub*」ソリューションの *Amazon S3* プラグインのアーキテクチャ

Amazon S3 プラグインは次のワークフローを実行します。

1. 時間ベースの Amazon EventBridge ルールで、AWS Fargate タスクを時間単位でトリガーして実行します。

2. AWS Fargate タスクで、送信元と送信先のバケットにあるすべてのオブジェクトをリストし、転送するオブジェクトを決定します。

3. AWS Fargate は、Amazon Simple Queue Service (Amazon SQS) に転送されるオブジェクトごとにメッセージを送信します。Amazon S3 イベントメッセージは、よりリアルタイムのデータ転送にも対応できます。送信元バケットにオブジェクトがアップロードされるたびに、同じ Amazon SQS キューにイベントメッセージが送信されます。

4. Amazon EC2 で実行されている JobWorker は、Amazon SQS のメッセージを使用し、オブジェクトを送信元バケットから送信先バケットに転送します。Auto Scaling グループを使用して、データを転送する Amazon EC2 インスタンスの数をビジネスニーズに基づいて制御できます。

5. 各オブジェクトの転送ステータスのレコードは、Amazon DynamoDB に保存されます。

6. Amazon EC2 インスタンスは、Amazon SQS メッセージに基づいて送信元バケットからオブジェクトを取得 (ダウンロード) します。

7. Amazon EC2 インスタンスは、Amazon SQS メッセージに基づいて送信先バケットにオブジェクトを配置 (アップロード) します。

注意: オブジェクト (またはオブジェクトの一部) の転送に失敗した場合、JobWorker はキュー内のメッセージを解放し、メッセージがキューに表示された後にオブジェクトを再度転送します (デフォルトの可視性タイムアウトは 15 分に設定されています)。転送が再度失敗した場合、メッセージはデッドレターキューに送信され、通知アラームが送信されます。

Amazon ECR プラグイン

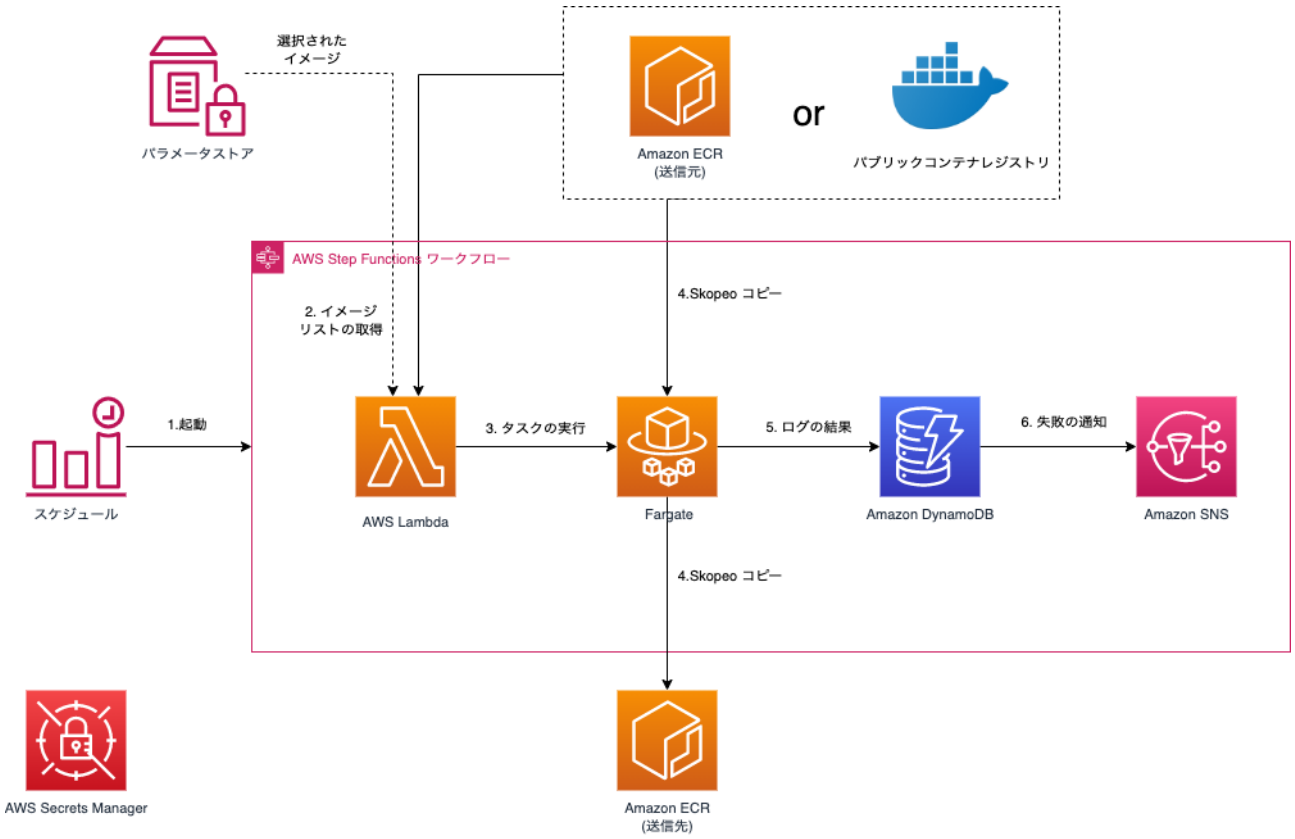

図 *3:* 「*Data Transfer Hub*」ソリューションの *Amazon ECR* プラグインのアーキテクチャ

Amazon ECR プラグインは次のワークフローを実行します。

1. Amazon EventBridge ルールで、AWS Step Functions ワークフローを定期的に実行します (デフォルトでは毎日実行されます)。
2. AWS Step Functions は、AWS Lambda を呼び出して送信元からイメージのリストを取得します。
3. AWS Lambda は、送信元の Amazon ECR のすべてのリポジトリコンテンツをリストするか、AWS Systems Manager Parameter Store から保存済みイメージリストを取得します。
4. 転送タスクは AWS Fargate 内で最大 10 個まで同時に実行されます。転送タスクが何らかの理由で失敗した場合は、自動的に 3 回再試行されます。

5. 各タスクで skopeo コピーを使用してターゲット Amazon ECR にイメージをコピーします。
6. コピーが完了すると、ステータス (成功または失敗) が追跡用に Amazon DynamoDB に記録されます。

ソリューションコンポーネント

このソリューションには、1) ウェブコンソール、2) Amazon S3 転送エンジン、3) Amazon ECR 転送エンジンの 3 つのコンポーネントがあります。

ウェブコンソール

このソリューションには、Amazon S3 と Amazon ECR の転送タスクを作成および管理できるシンプルなウェブコンソールが用意されています。

Amazon S3 転送エンジン

Amazon S3 転送エンジンは Amazon S3 プラグインを実行し、ソースから Amazon S3 バケットにオブジェクトを転送するために使用されます。Amazon S3 プラグインは、次の機能をサポートしています。

- AWS 中国リージョンと AWS リージョンの間での Amazon S3 のオブジェクトの転送
- Alibaba Cloud OSS/Tencent COS/Qiniu Kodo から Amazon S3 へのオブジェクトの転送
- Amazon S3 互換ストレージサービスから Amazon S3 へのオブジェクトの転送
- Amazon S3 イベントを介したほぼリアルタイムの転送
- オブジェクトメタデータを使用した転送
- 増分データの転送
- 自動再試行とエラー処理

Amazon ECR 転送エンジン

Amazon ECR エンジンは Amazon ECR プラグインを実行し、他のコンテナレジストリからコンテナイメージを転送するために使用されます。Amazon ECR プラグインは、次の機能をサポートしています。

- AWS 中国リージョンと AWS リージョンの間での Amazon ECR のイメージの転送
- パブリックコンテナレジストリ (Docker Hub、GCR.io、Quay.io など) から Amazon ECR への転送
- Amazon ECR への選択したイメージの転送
- Amazon ECR からのすべてのイメージとタグの転送

Amazon ECR プラグインは、基盤となるエンジンに skopeo を利用しています。AWS Lambda 関数でソース内のイメージをリストし、AWS Fargate を使用して転送ジョブを実行します。

セキュリティ

AWS インフラストラクチャでシステムを構築する場合、セキュリティ上の責任はお客様と AWS の間で共有されます。この責任共有モデルにより、AWS がホストオペレーティングシステムと仮想化レイヤーからサービスが運用されている施設の物理的なセキュリティに至るまでの要素を運用、管理、および制御するため、お客様の運用上の負担を軽減するのに役立ちます。AWS セキュリティの詳細については、「AWS クラウドセキュリティ」を参照してください。

IAM ロール

AWS Identity and Access Management (IAM) ロールにより、AWS クラウドのサービスとユーザーに対してアクセスポリシーとアクセス許可を詳細に割り当てることができます。このソリューションでは、AWS Lambda 関数、Amazon API Gateway、および Amazon Cognito に AWS リージョンのリソースを作成するためのアクセス権を付与する IAM ロールを作成します。

Amazon CloudFront

このソリューションでは、Amazon Simple Storage Service (Amazon S3) バケットでホストするウェブコンソールをデプロイします。レイテンシーを軽減し、セキュリティを向上させるために、このソリューションには、オリジンアクセスアイデンティティを持つ Amazon CloudFront ディストリビューションが含まれています。これは、このソリューションのウェブサイトバケットにあるコンテンツに、パブリックアクセスを提供する Amazon CloudFront ユーザーです。詳細については、*Amazon CloudFront* 開発者ガイドの「オリジンアクセスアイデンティティを使用して Amazon S3 コンテンツへのアクセスを制限する」を参照してください。

設計に関する考慮事項

デプロイ可能なリージョン

このソリューションでは、一部の AWS リージョンでは現在利用できないサービスを使用しています。このソリューションは必要なサービスが利用可能な AWS リージョンで起動してください。AWS リージョンで利用可能な AWS サービスの最新情報については、AWS リージョン別のサービスを参照してください。

AWS リージョンでデプロイがサポートされているリージョン

リージョン ID	リージョン名
us-east-1	米国東部 (バージニア北部)
us-east-2	米国東部 (オハイオ)
us-west-1	米国西部 (北カリフォルニア)
us-west-2	米国西部 (オレゴン)
ap-south-1	アジアパシフィック (ムンバイ)
ap-northeast-2	アジアパシフィック (ソウル)
ap-southeast-1	アジアパシフィック (シンガポール)
ap-southeast-2	アジアパシフィック (シドニー)
ap-northeast-1	アジアパシフィック (東京)
ca-central-1	カナダ (中部)
eu-central-1	欧州 (フランクフルト)
eu-west-1	欧州 (アイルランド)
eu-west-2	欧州 (ロンドン)
eu-west-3	欧州 (パリ)
eu-north-1	欧州 (ストックホルム)
sa-east-1	南米 (サンパウロ)

AWS 中国リージョンでデプロイがサポートされているリージョン

リージョン ID	リージョン名
cn-north-1	中国 (北京) リージョン (Sinnet が運営)
cn-northwest-1	中国 (寧夏) リージョン (NWCD が運営)

AWS CloudFormation テンプレート

デプロイを自動化するために、このソリューションでは次の AWS CloudFormation テンプレートが使用されており、デプロイ前にダウンロード可能です。

テンプレートを表示 **DataTransferHub-cognito.template:** このテンプレートは、Amazon Cognito を利用できる **AWS リージョン**でソリューションとすべての関連コンポーネントを起動するために使用します。デフォルト設定では、Amazon S3、Amazon CloudFront、AWS AppSync、Amazon DynamoDB、AWS Lambda、Amazon ECS、Amazon Cognito がデプロイされますが、特定のニーズに合わせてテンプレートをカスタマイズできます。

テンプレートを表示 **DataTransferHub-openid.template:** このテンプレートは、Amazon Cognito を**利用できない AWS 中国リージョン**でソリューションとすべての関連コンポーネントを起動するために使用します。デフォルト設定では、Amazon S3、Amazon CloudFront、AWS AppSync、Amazon DynamoDB、AWS Lambda、Amazon ECS がデプロイされますが、特定のニーズに合わせてテンプレートをカスタマイズできます。

自動デプロイ

このソリューションを起動する前に、コスト、アーキテクチャ、ネットワークセキュリティなど、このガイドで説明されている考慮事項を確認してください。このセクションの手順に従って、このソリューションを設定して AWS アカウントにデプロイします。

デプロイ時間: 約 15 分

デプロイの概要

次の手順を使用して、このソリューションを AWS にデプロイします。手順の詳細については、各ステップのリンクを参照してください。

ステップ 1. スタックの起動

- (オプション 1) AWS リージョンで AWS CloudFormation テンプレートをデプロイする
- (オプション 2) AWS 中国リージョンで AWS CloudFormation テンプレートをデプロイする

ステップ 2. ウェブコンソールを起動する

ステップ 3. 転送タスクを作成する

ステップ 1. (オプション 1) AWS リージョンでのスタックの起動

> **重要:** 次のデプロイ手順は、AWS リージョンにのみ適用されます。AWS 中国リージョンでのデプロイについては、オプション 2 を参照してください。

前提条件

新しい AWS アカウントで初めてデプロイする場合は、AWS AppSync のサービスにリンクされたロールが存在しない可能性があります。ロールを作成するには、CloudShell で次のコマンドを実行する必要があります。

```
aws iam create-service-linked-role --aws-service-
name appsync.amazonaws.com
```

AWS CloudFormation テンプレートのデプロイ (オプション 1 – AWS リージョン)

この自動化された AWS CloudFormation テンプレートは、AWS クラウドに「Data Transfer Hub」ソリューションをデプロイします。スタックを起動する前に、前提条件の操作を済ませておく必要があります。

> **注意:** このソリューションの実行中に使用した AWS のサービスのコストは、お客様の負担となります。詳細については、このガイドの「コスト」セクションに移動し、このソリューションで使用する AWS のサービス別の料金ウェブページを参照してください。

1. AWS マネジメントコンソールにサインインして、`DataTransferHub-cognito.template` AWS CloudFormation テンプレートを起動するボタンを選択します。または、独自にカスタマイズするためにテンプレートをダウンロードすることもできます。

   ソリューションの起動

2. このテンプレートは、デフォルトで米国東部 (バージニア北部) リージョンで起動されます。別の AWS リージョンでこのソリューションを起動するには、コンソールのナビゲーションバーのリージョンセレクターを使用します。
3. **スタックの作成**ページで、正しいテンプレート URL が **Amazon S3 URL** テキストボックスに示されていることを確認し、[**次へ**]を選択します。
4. **スタックの詳細を指定**ページで、このソリューションのスタックに名前を割り当てます。名前の文字数制限に関する詳細は、*AWS Identity and Access Management* ユーザーガイドの「IAM および AWS STS クォータ」を参照してください。
5. **パラメータ**で、このソリューションのテンプレートのパラメータを確認し、必要に応じて変更します。このソリューションでは、次のデフォルト値を使用します。

パラメータ	デフォルト	説明
AdminEmail	<入力が必須>	管理者ユーザーの E メール。

6. [**次へ**] を選択します。
7. **スタックオプションの設定**ページで、デフォルト値のまま [**次へ**] を選択します。
8. **レビュー**ページで、設定を確認します。テンプレートで AWS Identity and Access Management (IAM) リソースを作成することを承認するチェックボックスを必ずオンにします。
9. [**スタックの作成**] を選択してスタックをデプロイします。

   スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 15 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 1. (オプション 2) AWS 中国リージョンでスタックを起動する

> **重要:** 次のデプロイ手順は、AWS 中国リージョンにのみ適用されます。AWS リージョンでのデプロイについては、オプション 1 を参照してください。

前提条件

1. OIDC ユーザープールを作成します。
2. ドメインネームサービス (DNS) の解決を設定します。

前提条件 1: OIDC ユーザープールの作成

Amazon Cognito がまだ利用できない AWS リージョンでは、OIDC を使用して認証を提供できます。次の手順では AWS パートナーの Authing を例として使用しますが、利用可能な任意のプロバイダーを選択することもできます。

1. Authing 開発者アカウントにサインアップします。詳細については、「How to register an account」(中文) を参照してください。
2. Authing にサインインします。
3. [**Create new user pool**] を選択し、名前を入力して [**Confirm**] を選択します。
4. ユーザープールが作成されたら、OIDC 認証用のアプリケーションを作成できます。
    a. **Application** から [**Configuration**] を選択し、[**Basic Settings**] を選択します。
    b. プロトコルのタイプが OIDC であることを確認します。
5. 認証設定を更新します。
    a. **Application** から [**Configuration**] を選択し、[**Authorization configuration**] を選択します。
    b. 認証フローを **implicit** に更新し、戻り型を **id_token** に更新します。

c. id_token 署名アルゴリズムで [**RS256**] を選択します。

d. [**Save**] を選択します。

6. コールバック URL を更新します。

a. **Application** から [**Configuration**] を選択し、[**Auth Config**] を選択します。

b. ログインコールバック URL を `https://<your-custom-domain>/authentication/callback` に変更します。

c. [**Save**] を選択します。

> **注意**: 中国でドメイン名の ICP 登録が完了していることを確認してください。

7. ログイン制御を更新します。

a. **Application** から [**Login control**] を選択し、[**Registration and Login**] を選択します。

b. **Email** と **Phone** のチェックボックスをオフにして、すべての登録方法を無効にします。

c. [**Save**] を選択します。

8. 管理者ユーザーを作成します。

a. **Users & Roles** から [**Users**] を選択し、[**Create user**] を選択します。

b. ユーザーの E メールを入力します。

c. [**OK**] を選択します。

d. E メールで一時パスワードを確認します。

e. ユーザーパスワードをリセットします。

> **注意**: このソリューションはアプリケーションロールをサポートしていないため、すべてのユーザーに管理者権限が付与されます。

前提条件 2: ドメインネームサービスの解決を設定

ICP ライセンスのドメインが Amazon CloudFront のデフォルトのドメイン名を指すように、ドメインネームサービス (DNS) の解決を設定します。オプションで、独自の DNS リゾルバーを使用できます。

Amazon Route 53 の設定例を次に示します。

1. Amazon Route 53 でホストゾーンを作成します。詳細については、「Amazon Route 53 開発者ガイド」を参照してください。
2. コンソールの URL の CNAME レコードを作成します。
   a. ホストゾーンから [**レコードの作成**] を選択します。
   b. **レコード名**入力ボックスにホスト名を入力します。
   c. **レコードタイプ**から [**CNAME**] を選択します。
   d. 値フィールドに AWS CloudFormation の出力タブにある **PortalUrl** を入力します。
   e. [**レコードを作成**] を選択します。
3. Amazon CloudFront ディストリビューションに代替ドメイン名を追加します。
   a. Amazon CloudFront コンソールを開くように Amazon CloudFront の対応するドメイン名を設定します。そのためには、リストで PortalURL のディストリビューション ID を見つけて [**ID**] を選択します (または、チェックボックスをオンにして [**ディストリビューション設定**] を選択します)。

ディストリビューションを編集し、代替ドメイン名 (CNAME) に Amazon Route 53 のレコードを追加します。

AWS CloudFormation テンプレートのデプロイ (オプション 2 – AWS 中国リージョン)

この自動化された AWS CloudFormation テンプレートは、AWS クラウドに「Data Transfer Hub」ソリューションをデプロイします。スタックを起動する前に、ODIC ユーザープールを作成し、DNS の解決を設定する必要があります。

> **注意:** このソリューションの実行中に使用した AWS のサービスのコストは、お客様の負担となります。詳細については、このガイドの「コスト」セクションに移動し、このソリューションで使用する AWS のサービス別の料金ウェブページを参照してください。

1. AWS マネジメントコンソールにサインインして、`DataTransferHub-openid.template` AWS CloudFormation テンプレートを起動するボタンを選択します。または、独自にカスタマイズするためにテンプレートをダウンロードすることもできます。

2. テンプレートはコンソールのデフォルトの AWS リージョンで起動します。別の AWS リージョンでこのソリューションを起動するには、コンソールのナビゲーションバーのリージョンセレクターを使用します。
3. **スタックの作成**ページで、正しいテンプレート URL が **Amazon S3 URL** テキストボックスに表示されていることを確認し、[**次へ**] を選択します。
4. **スタックの詳細を指定**ページで、このソリューションのスタックに名前を付けます。名前の文字数制限に関する詳細は、*AWS Identity and Access Management* ユーザーガイドの「IAM および AWS STS クォータ」を参照してください。
5. **パラメータ**で、このソリューションのテンプレートのパラメータを確認し、必要に応じて変更します。このソリューションでは、次のデフォルト値を使用します。

パラメータ	デフォルト	説明
OidcProvider	<入力が必須>	OIDC アプリケーション設定に表示される発行者を参照します。
OidcClientId	<入力が必須>	OIDC アプリケーション設定に表示されるアプリ ID を参照します。
OidcCustomerDomain	<入力が必須>	Authing が提供するサブドメインではなく、中国で ICP 登録を完了したお客様のドメインを参照します。`https://` で始まる必要があります。

6. [**次へ**] を選択します。
7. **スタックオプションの設定**ページで、デフォルト値のまま [**次へ**] を選択します。
8. **レビュー**ページで、設定を確認します。テンプレートで AWS Identity and Access Management (IAM) リソースを作成することを承認するチェックボックスを必ずオンにします。

9. [**スタックの作成**] を選択してスタックをデプロイします。

   スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 15 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 2. ウェブコンソールを起動する

スタックが正常に作成されたら、AWS CloudFormation の**出力**タブに移動し、**PortalUrl** の値を選択して「Data Transfer Hub」ソリューションのウェブコンソールにアクセスします。

ウェブコンソールへのログイン

「Data Transfer Hub」ソリューションにログインして設定するオプションは、ソリューションがデプロイされた場所に応じて 2 通りあります。

1. Amazon Cognito ユーザープールでログイン (AWS リージョンの場合)
2. Authing.cn を使用して OpenID でログイン (AWS 中国リージョンの場合)

デプロイが成功すると、一時ログインパスワードを含む E メールが指定の E メールアドレスに送信されます。

AWS リージョンの Amazon Cognito ユーザープールによるログイン

1. ウェブブラウザを使用して、AWS CloudFormation の**出力**タブから **PortalURL** を入力し、Amazon Cognito コンソールに移動します。
2. **AdminEmail** と一時パスワードを使用してサインインします。
   a. 新しいアカウントパスワードを設定します。
   b. (オプション) アカウントの復旧用に E メールアドレスを検証します。
3. 検証が完了すると、「Data Transfer Hub」ソリューションのウェブコンソールが開きます。

(オプション 2) AWS 中国リージョンの OpenID 認証

1. ウェブブラウザを使用して、「Data Transfer Hub」ソリューションのドメイン名を入力します。

a. 初めてログインする場合、Authing.cn ログインインターフェイスが開きます。

2. ソリューションのデプロイ時に登録したユーザー名とパスワードを入力し、[**ログイン**] を選択します。「Data Transfer Hub」ソリューションのウェブコンソールが開きます。

3. パスワードを変更し、再度サインインします。

ステップ 3. 転送タスクを作成する

ウェブコンソールを使用して、Amazon S3 または Amazon ECR の転送タスクを作成します。

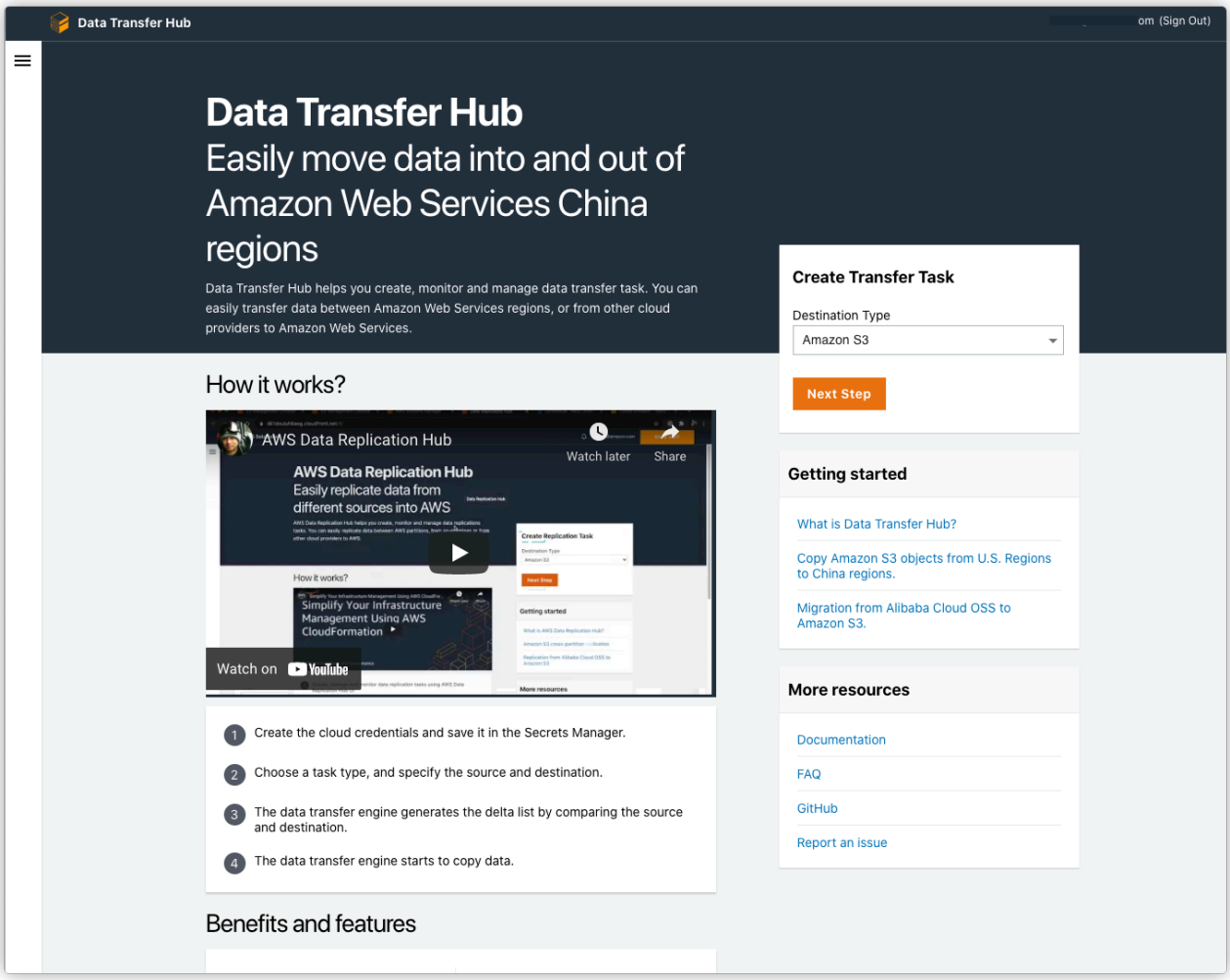

図 *3: 「Data Transfer Hub」ソリューションのウェブコンソール*

Amazon S3 転送タスクの作成

1. **Create Transfer Task** ページで、[**Amazon S3**] を選択し、[**Next Step**] を選択します。
2. **Engine options** ページで、エンジンの下の [**Amazon S3**] を選択し、[**Next Step**] を選択します。
3. 転送タスクの詳細を指定します。
   a. **Source Type** で、データソースを選択します (例: **Amazon S3**)。
4. リクエストの **Source settings** を入力します。**Input bucket name** と **object prefix** (オプション) を指定します。

   データの送信元バケットが「Data Transfer Hub」ソリューションのデプロイ先のアカウントにある場合は、**Yes** を選択し、Amazon S3 イベントによるデータ転送のトリガーを許可します。

   送信元バケットが「Data Transfer Hub」ソリューションのデプロイ先と同じアカウントにない場合は、**No** を選択し、送信元バケットの認証情報を指定します。

   認証情報を作成するには、[**Secrets Manager**] を選択して現在のリージョンの AWS Secrets Manager コンソールに移動します。

   a. 左側のメニューから [**シークレット**] を選択し、[**新しいシークレットを保存する**] を選択して、[**その他のシークレットのタイプ**] キータイプを選択します。

   b. 表示された形式に従って、**プレーンテキスト**入力ボックスに *access_key_id* と *secret_access_key* の情報を入力します。詳細については、*AWS IAM* ユーザーガイドの「IAM の機能」を参照してください。[**次へ**] を選択します。

   c. (オプション) キーの名前と説明を入力します。[**次へ**] を選択します。

   d. 自動ローテーションの設定で、[**自動ローテーションの無効**] を選択します。[**次へ**] を選択します。

   e. デフォルト値のまま [**保存**] を選択してキーの作成を完了します。

f.「Data Transfer Hub」ソリューションのタスク作成インターフェイスに戻り、インターフェイスを更新します。新しいシークレットがドロップダウンリストに表示されます。

g. 証明書 (シークレット) を選択します。

5. Amazon S3 バケットの送信先設定を指定します。

   Amazon S3 の送信元バケットが「Data Transfer Hub」ソリューションのデプロイ先と同じアカウントにある場合は、**destination settings** で Amazon S3 の送信先バケットの認証情報を作成または指定する必要があります。それ以外の場合、認証情報は必要ありません。次の手順を使用して送信先の設定を更新します。

   a. **Engine settings** で値を確認し、必要に応じて変更します。増分データ転送の場合は、最小容量を少なくとも `1` に設定することをお勧めします。

   b. **Advanced Options** はデフォルト値のままにします。

   c. **More** タブで追加情報を入力します。**Alarm Email** で E メールアドレスを指定する必要があります。

6. [**Next**] を選択し、タスクパラメータの詳細を確認します。

7. [**Create Task**] を選択します。

   タスクが正常に作成されると、**Tasks** ページに表示されます。

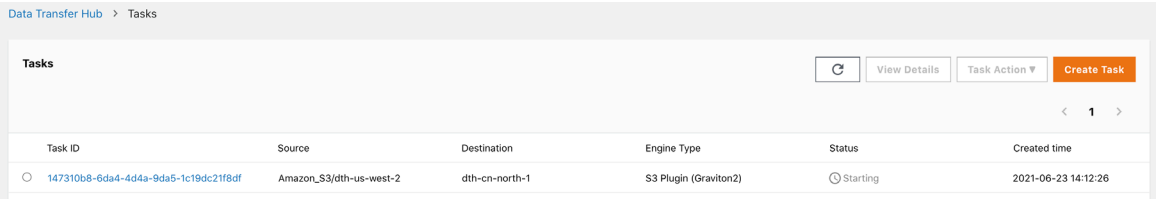

図 *4:* 転送タスクの詳細とステータス

[**Task ID**] を選択してタスクの **Details** ページに移動し、[**CloudWatch Dashboard**] を選択してタスクのステータスを監視します。

Amazon ECR 転送タスクの作成

1. **Create Transfer Task** ページで、[**Amazon ECR**] を選択し、[**Next Step**] を選択します。
2. 転送タスクの詳細を指定します。
    a. **Source Type** で、コンテナレジストリタイプを選択します。
    b. **Source settings** で、送信元のリージョン名とアカウント ID を入力します。認証情報を作成するには、[**Secrets Manager**] を選択して現在のリージョンの AWS Secrets Manager コンソールに移動します。
        1. 左側のメニューから [**シークレット**] を選択し、[**新しいシークレットを保存する**] を選択して、[**その他のシークレットのタイプ**] キータイプを選択します。
        2. 表示された形式に従って、**プレーンテキスト**入力ボックスに *access_key_id* と *secret_access_key* の情報を入力します。詳細については、*AWS IAM* ユーザーガイドの「IAM の機能」を参照してください。[**次へ**] を選択します。
        3. (オプション) キーの名前と説明を入力します。[**次へ**] を選択します。
        4. 自動ローテーションの設定で、[**自動ローテーションの無効**] を選択します。[**次へ**] を選択します。
        5. デフォルト値のまま [**保存**] を選択してキーの作成を完了します。
        6. 「Data Transfer Hub」ソリューションのタスク作成インターフェイスに戻り、インターフェイスを更新します。新しいシークレットがドロップダウンリストに表示されます。
        7. 証明書 (シークレット) を選択します。
        8. 送信先の設定を指定します。

    送信元が「Data Transfer Hub」ソリューションのデプロイ先と同じアカウントにある場合は、送信先の認証情報を作成または指定する必要があります。それ以外の場合、認証情報は必要ありません。

a. **More** セクションで追加情報を入力します。**More** タブで追加情報を入力します。**Alarm Email** で E メールアドレスを指定する必要があります。

3. [**Next**] を選択し、タスクパラメータの詳細を確認します。
4. [**Create Task**] を選択します。

   タスクが正常に作成されたら、**Tasks** ページでタスクのステータスを確認できます。

その他のリソース

- AWS CloudFormation
- Amazon S3
- AWS Lambda
- AWS Step Functions
- Amazon CloudFront
- Amazon ECR
- Amazon DynamoDB
- AWS AppSync
- Amazon Cognito
- AWS IAM
- Amazon EC2
- Amazon Route 53

ソリューションのアンインストール

「Data Transfer Hub」ソリューションは、AWS マネジメントコンソールから、または AWS Command Line Interface を使用してアンインストールできます。アンインストールする前に、アクティブな転送タスクを手動で停止する必要があります。

AWS マネジメントコンソールの使用

1. AWS CloudFormation コンソールにサインインします。
2. **スタック**ページで、このソリューションをインストールしたスタックを選択します。
3. [**削除**] を選択します。

AWS Command Line Interface の使用

AWS Command Line Interface (AWS CLI) がお客様の環境で使用できるかどうかを確認します。インストール手順については、*AWS CLI* ユーザーガイドの「AWS Command Line Interface とはどのようなものですか」を参照してください。AWS CLI が使用できることを確認したら、次のコマンドを実行します。

```
$ aws cloudformation delete-stack --stack-name <installation-stack-name>
```

Amazon S3 バケットの削除

このソリューションは、誤ってデータを損失しないように、AWS CloudFormation スタックを削除しても、このソリューションで作成された Amazon S3 バケットが (AWS オプトインリージョンへのデプロイ目的で) 保持されるように設定されています。このソリューションをアンインストールした後に、データを保持する必要がない場合は、Amazon S3 バケットを手動で削除できます。次の手順に従って、Amazon S3 バケットを削除してください。

1. Amazon S3 コンソールにサインインします。
2. 左のナビゲーションペインから [**バケット**] を選択します。
3. *<stack-name>* Amazon S3 バケットを見つけます。
4. その Amazon S3 バケットを選択し、[**削除**] を選択します。

AWS CLI を使用して Amazon S3 バケットを削除するには、次のコマンドを実行してください。

```
$ aws s3 rb s3://<bucket-name> --force
```

ソースコード

GitHub リポジトリにアクセスして、このソリューションのソースファイルをダウンロードし、カスタマイズを他のユーザーと共有できます。「Data Transfer Hub」ソリューションのテンプレートは、AWS Cloud Development Kit (AWS CDK) を使用して生成されます。詳細については、README.md ファイルを参照してください。

ドキュメントの改訂

日付	変更
2022 年 1 月	初回リリース

寄稿者

- Aiden Dai
- Kervin Hu
- Haiyun Chen
- Joe Shi
- Ashwini Rudra
- Jyoti Tyagi

注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。このドキュメントは、(a) 情報提供のみを目的としており、(b) AWS の現行製品とプラクティスを表したものであり、予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約義務や確約を意味するものではありません。AWS の製品やサービスは、明示または暗示を問わず、いかなる保証、表明、条件を伴うことなく「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

「Data Transfer Hub」ソリューションは、Classless Inter-Domain Routing (CIDR) で閲覧可能な Apache ライセンスバージョン 2.0 の条項に基づいてライセンスされます。