

AWS re:Invent 2024 で発表された AWS Transfer Family web appsを 触ってみた

2025/01/15 Serverless LT初心者向け LT大会 #50

高寺香次



社外のコミュニティ
初登壇です！

よろしくお願いします！



Profile

高寺 香次 (たかてらこうじ)

NECソリューションイノベータ株式会社

3年目

趣味：カラオケ、ドライブ、ブログ



各種SNS

昨年12月のAWS re:Invent 2024に参加してきました！



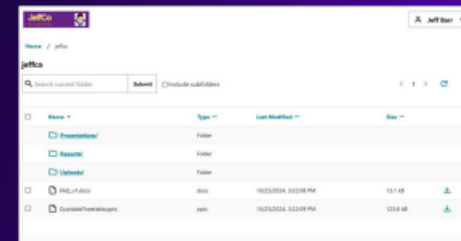
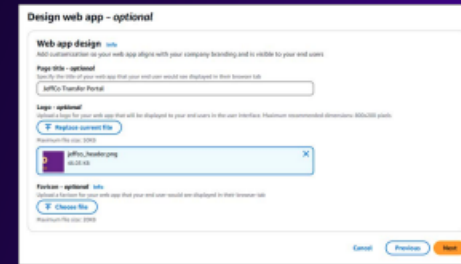
■ AWS re:Inventとは？

- ・ AWSが毎年ラスベガスで開催する学習型カンファレンス
- ・ 数多くのサービスアップデートが発表される
2024年は100件以上
- ・ 様々なコンテンツに参加可能
 - ・ Keynote
 - ・ WorkShop
 - ・ Jam/GameDay
 - ・ Chalk Talk etc.

AWS Transfer Family web apps を触ってみました

AWS Transfer Family web appsを発表

- S3のデータを参照・アップロード・ダウンロードするためのポータルサイトをフルマネージドで提供
- IT部門以外のユーザがManagement Consoleに触れることなくS3のファイル进行操作できる
- ページのタイトルとfaviconがカスタマイズでき、CloudFrontを組み合わせることでカスタムドメインでの運用にも対応
- 権限管理はIAM Identity Centerで行う。SAMLやOIDC連携もサポートする
- 東京含む9リージョンで利用可能に

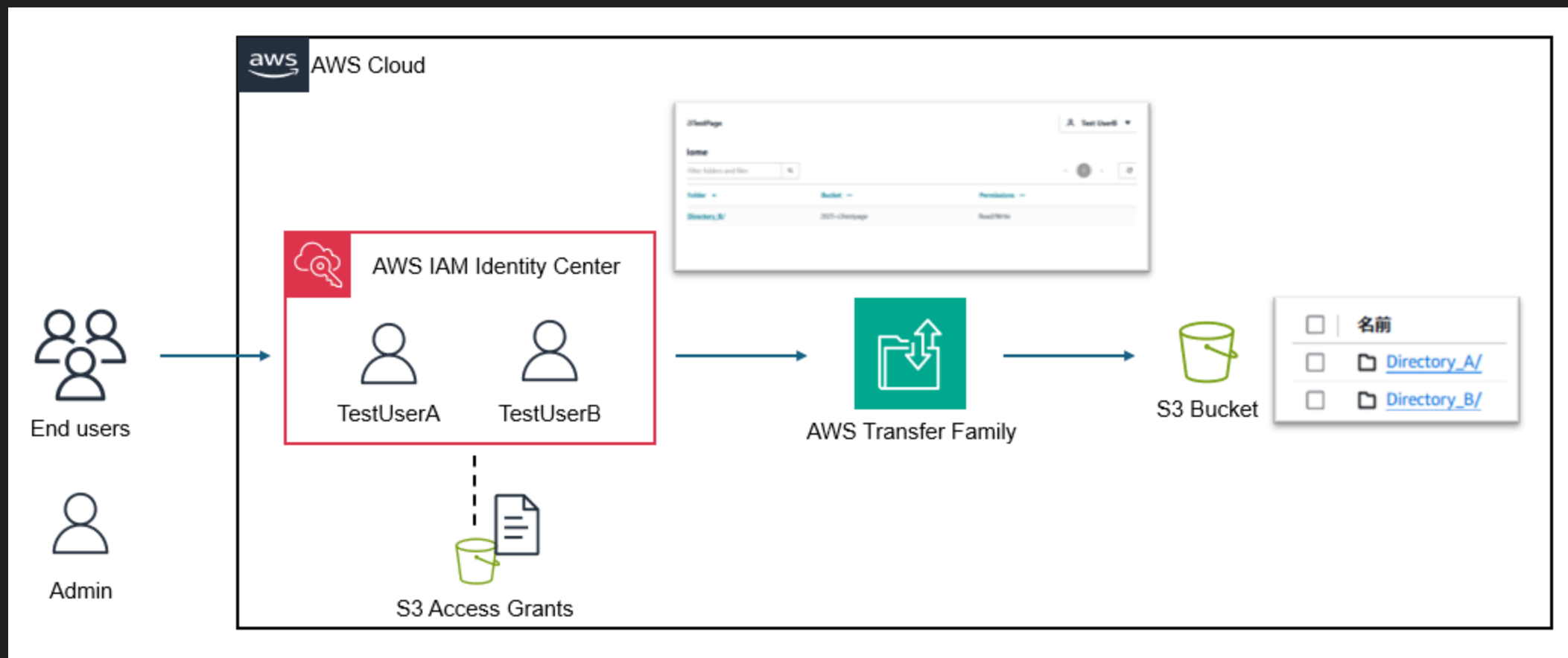


© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

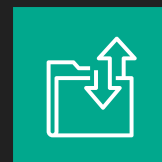
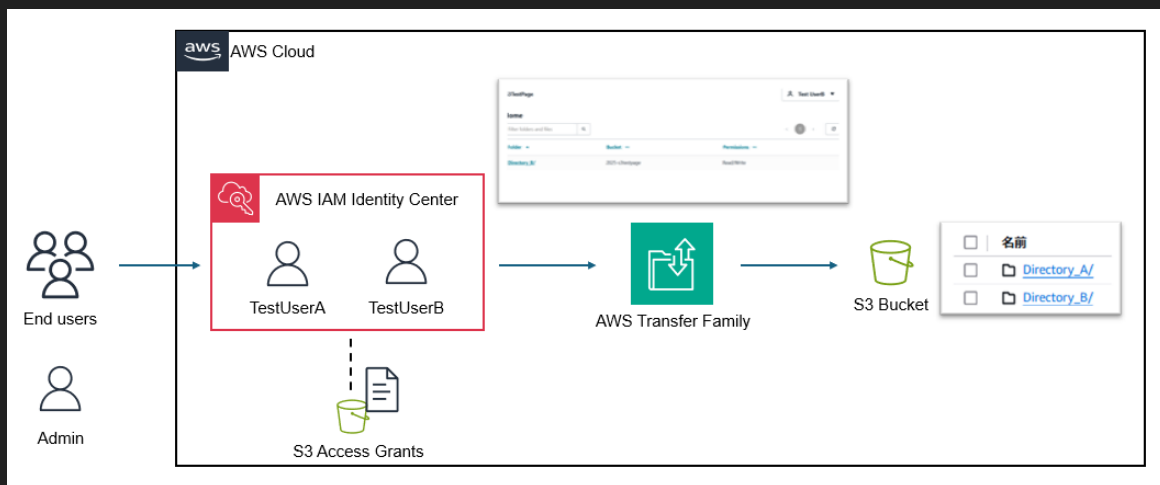
#AWSDevLiveShow 113

引用 : <https://aws.amazon.com/jp/blogs/news/2024-12-reinvent2024-aws-blackbelt/>

構成図



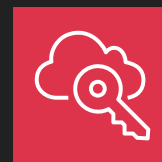
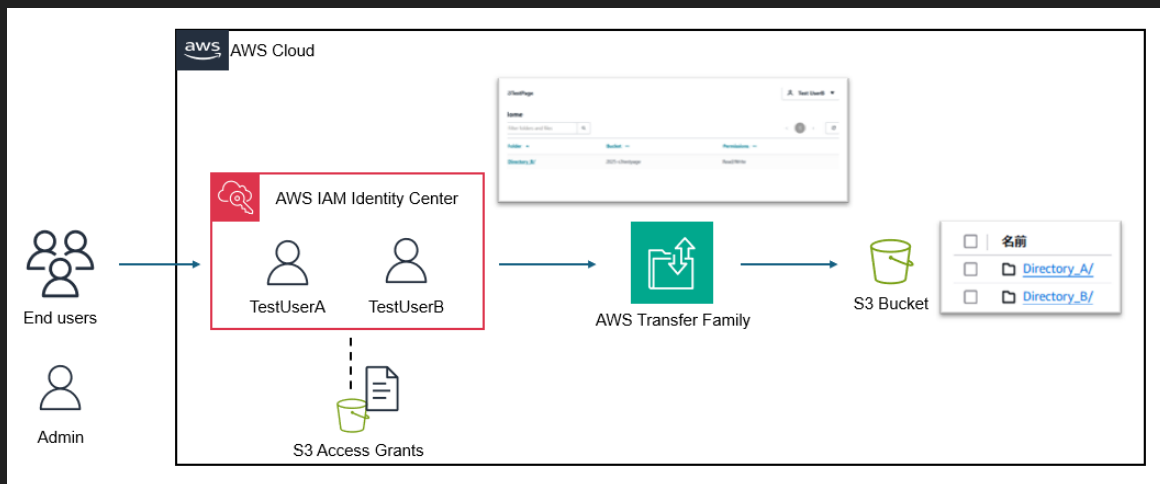
各サービス・機能概要について



AWS Transfer Family

- ・フルマネージド型のファイル転送サービス
- ・SFTP、FTPS、FTP、およびAS2経由でAWSストレージサービスと直接ファイル転送が可能
- ・容量制限がないS3/EFSをストレージとして利用

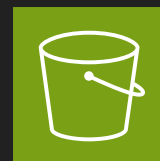
各サービス・機能概要について



AWS IAM Identity Center

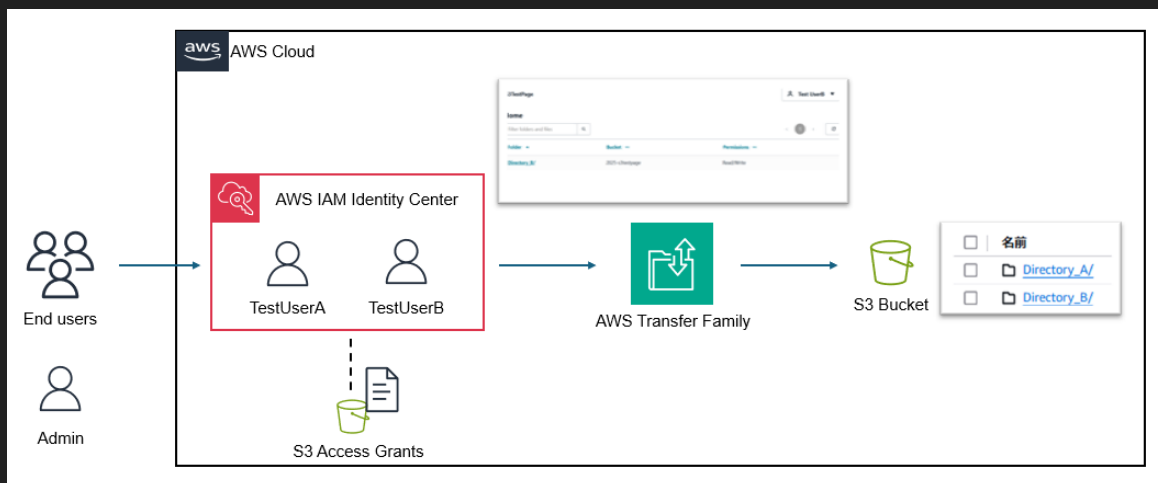
- ・ ユーザーをAWSマネージドアプリケーションやその他のAWSリソースに接続するためのサービス
- ・ 既存のIDプロバイダを接続して、そこからユーザーやグループの情報を同期可能
- ・ Identity Center内で直接ユーザー作成して管理することも可能

各サービス・機能概要について



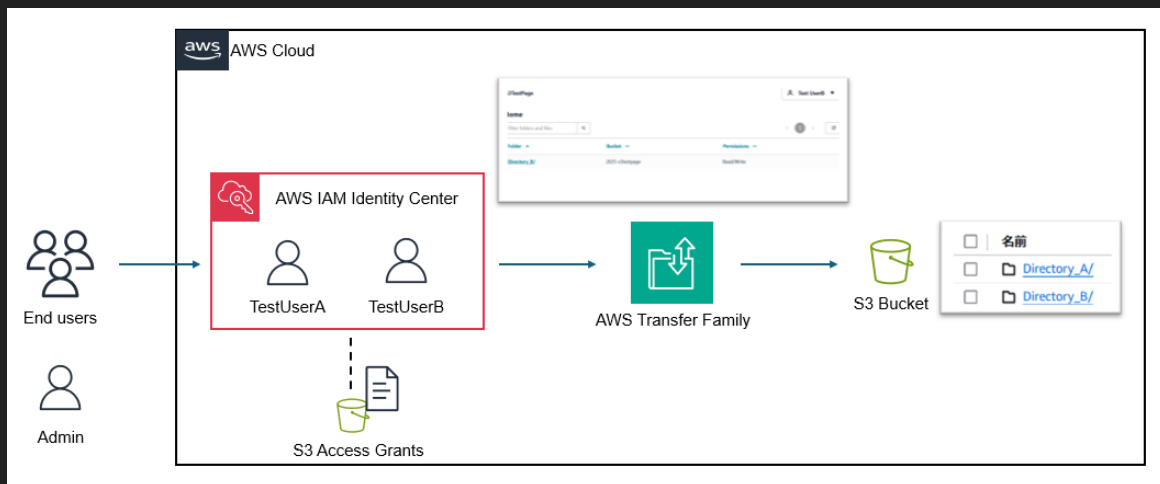
Amazon Simple Storage Service (Amazon S3)

- ・ AWSのオブジェクトストレージサービス
- ・ データ追加や削除に合わせて自動的に拡大縮小する
- ・ 99.999999999%のデータ耐久性と99.99%の可用性を提供する



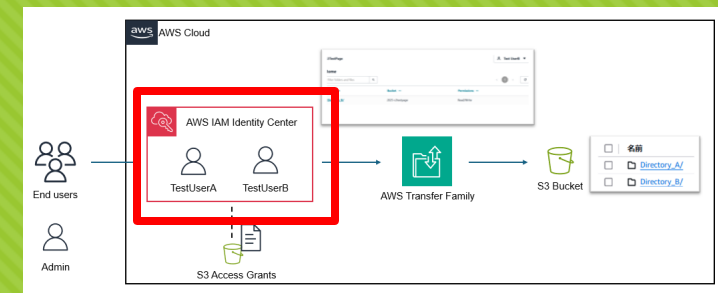
※今回は予め作成した状態で説明します

各サービス・機能概要について



- Amazon S3のアクセスコントロール機能
- S3内のデータアクセス許可をプレフィックス、バケット、オブジェクトごとに定義可能
- 企業内ディレクトリ等のIdPと連携し、S3へのアクセス権を付与可能

① IAM Identity Center の設定



ステップ 1
● ユーザーの詳細を指定

ステップ 2 - 任意
ユーザーをグループに追加

ステップ 3
ユーザーの確認と追加

ユーザーの詳細を指定

プライマリ情報

ユーザー名
このユーザー名は、このユーザーが AWS access portal にサインインするために必要です。ユーザー名は後で変更することはできません。

TestUserA

最大長は 128 文字です。英数字または +、@、- のいずれかを使用できます。

パスワード
このユーザーがパスワードを受け取る方法を選択します。 [詳細はこちら](#)

☒ パスワードの設定手順が記載された E メールをこのユーザーに送信します。

☐ このユーザーと共有できるワンタイムパスワードを生成します。

E メールアドレス

E メールアドレスを確認

名

Test

姓

U5er

表示名
これは通称。ワークフォースユーザーのフルネーム (姓名) で、検索可能であり、ユーザーリストに表示されます。

Test U5erA

ユーザー (2)

ここに一覧表示されているユーザーは、AWS access portal にサインインして、AWS アカウントと割り当てられたクラウドアプリケーションにアクセスできます。 [詳細はこちら](#)

ユーザー名 ▼

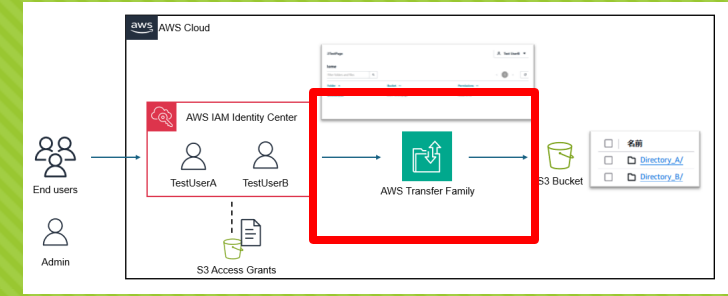
Q ユーザーを検索

ユーザーを削除 ユーザーを追加

☐	ユーザー名	表示名	ステータス	MFA デバイス	作成者
☐	TestUserA	Test UserA	有効	なし	手動
☐	TestUserB	Test UserB	有効	なし	手動

IAM Identity Centerでユーザーを作成

② Transfer Family web apps の作成



ステップ1
● Web アプリの設定
○ ステップ2 - オプション
○ ウェブアプリのデザイン
○ ステップ3
○ 確認と作成

Web アプリの設定

認証アクセス 情報
アイデンティティセンターインスタンスを接続または作成します。

● お客様の AWS Transfer Family アプリケーションが IAM Identity Center に接続されています
お客様の AWS Transfer Family アプリケーションへのアクセスを管理するには、IAM Identity Center 内のユーザーとグループをこのアプリケーションに割り当てます。 [詳細はこちら](#)

権限タイプ 情報
● 新しいサービスロールを作成して使用する
IAM ロールを作成して使用すると、アプリケーションの作成に必要な AWS リソースにサービスがアクセスできるようになります。
○ 既存のロールを使用
既存の IAM ロールを使用して、アプリケーションの作成に必要な AWS リソースにサービスがアクセスできるようになります。

ウェブアプリユニット 情報
必要な同時接続数、または同時にウェブアプリで実行されるユーザーセッション数に必要なユニット数を選択します。を参照してください。 [価格設定ページ](#)

1 (最大 250 つの同時セッション)

タグ
タグを使用して、ウェブアプリを整理、検索、フィルタリングできます。ウェブアプリを簡単に識別できるように、キーに「名前」、値に一意の文字列を指定したタグを追加することをお勧めします。
リソースに関連付けられたタグはありません。

[タグを追加](#)
最大 50 個のタグをさらに追加できます。

[キャンセル](#) [次へ](#)

ステップ1
● Web アプリの設定
● ステップ2 - オプション
● ウェブアプリのデザイン
○ ステップ3
○ 確認と作成

ウェブアプリのデザイン - オプション

ウェブアプリのデザイン 情報
ウェブアプリが会社のブランドと合致し、エンドユーザーに表示されるようにカスタマイズを加えてください。

ページタイトル・オプション
エンドユーザーがブラウザタブに表示するウェブアプリのタイトルを指定します。

S3TestPage

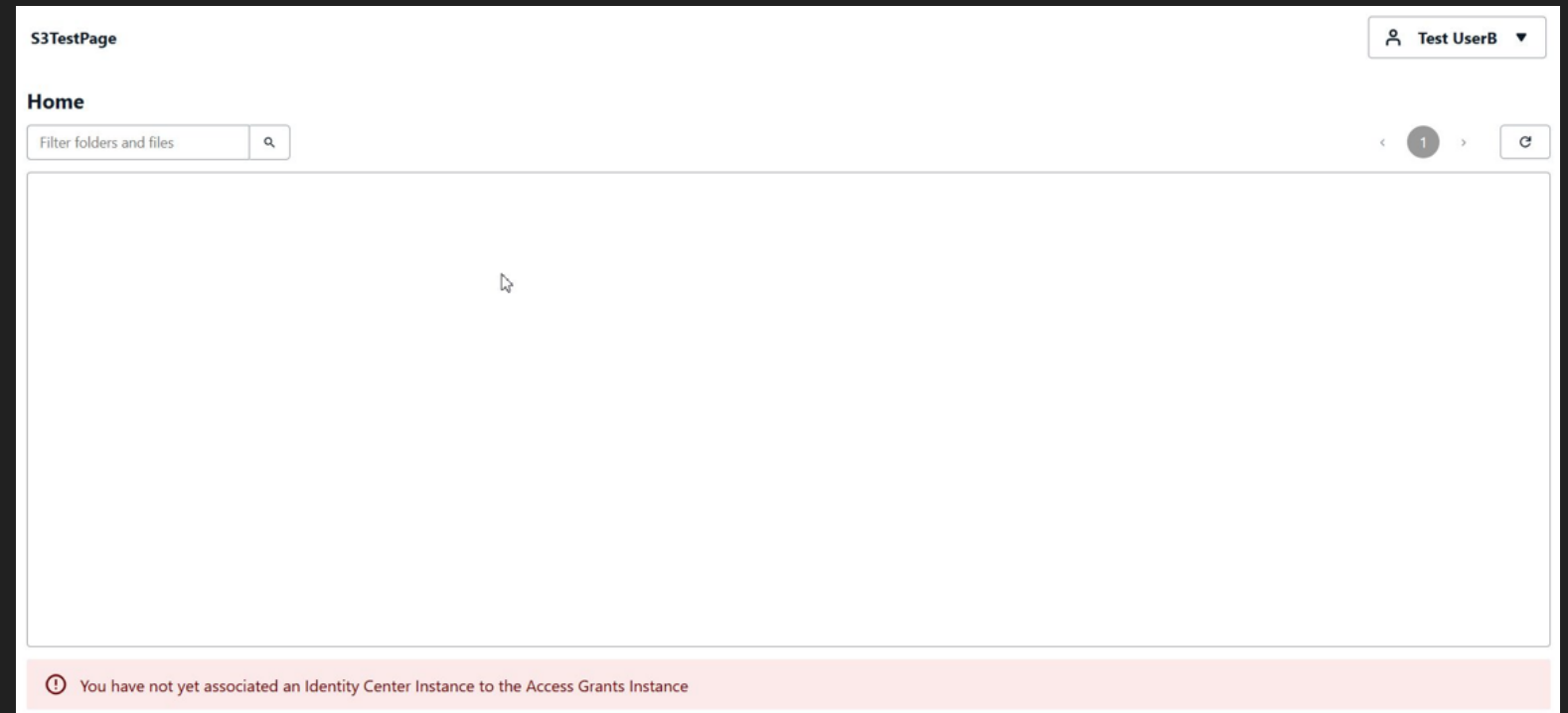
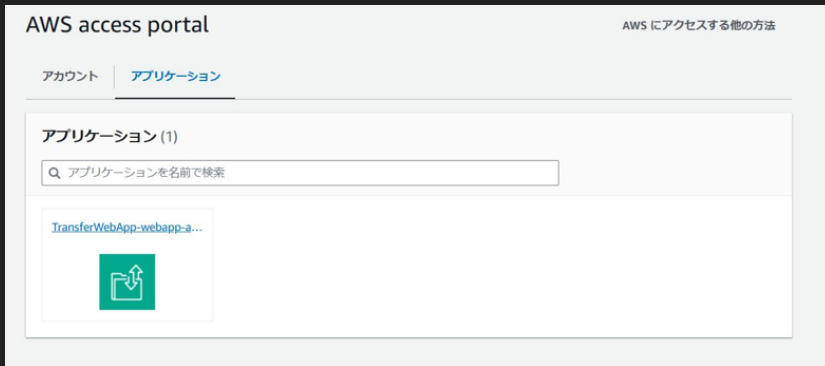
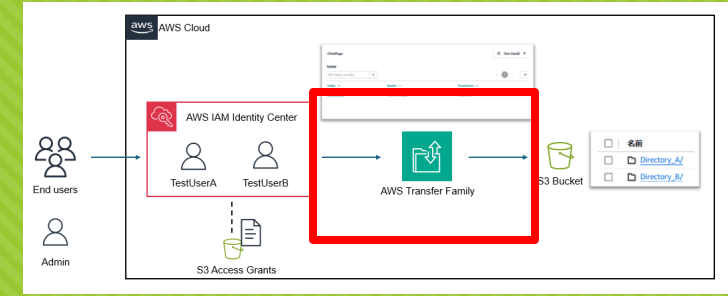
ロゴ・オプション
ウェブアプリのロゴをアップロードして、エンドユーザーにユーザーインターフェイスに表示します。推奨最大サイズ: 800x200 ピクセル。
[ファイルを選択](#)
最大ファイルサイズ: 50KB

ファビコン・オプション 情報
エンドユーザーのブラウザタブに表示されるウェブアプリのファビコンをアップロードします。
[ファイルを選択](#)
最大ファイルサイズ: 20KB

[キャンセル](#) [戻る](#) [次へ](#)

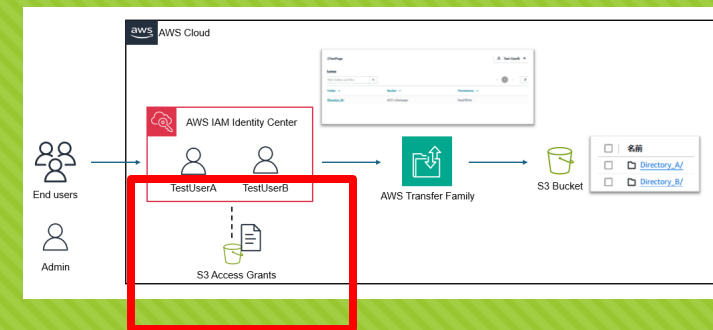
Transfer Family web appsを作成（ロゴ、ファビコンは今回はスキップ）

② Transfer Family web apps の作成



作成したユーザーでログイン。まだS3へのアクセス権がない状態

③ S3 Access Grants の設定



ロケーションを登録 [情報](#)

S3 のロケーションを登録すると、S3 Access Grants インスタンスは、指定された範囲内のリソースにアクセスするための一時的な認証情報を取得する許可を IAM ロールに割り当てます。

ロケーション [情報](#)

ロケーション範囲 [情報](#)

ロケーションを登録した後は、ロケーション範囲を編集することはできません。

範囲

[表示](#) [S3 の参照](#)

すべてのバケットの形式: s3://
バケットの形式: s3://
プレフィックスの形式: s3:///

許可

この IAM ロールは、S3 Access Grants が指定されたロケーション範囲にアクセスすることを許可します。

① ロケーション範囲にアクセスするための適切な許可がロールにあることを確認するには、[許可のリスト](#) を参照してください。

IAM ロール [情報](#)

この IAM ロールにより、S3 Access Grants は指定されたロケーション範囲にアクセスできます。

☐ 新しいロールの作成

☒ 既存の IAM ロールから選択

☐ IAM ロールの ARN を入力

既存の IAM ロールから選択

S3 アクセス権限は、この IAM ロールを引き受けてロケーションへのアクセスを管理します。

[表示](#)

[キャンセル](#) [ロケーションを登録](#)

許可とアクセス

ユーザーまたはロールに、S3 データに対する特定のレベルのアクセス権を付与します。

⚠️ S3 コンソールを使用して、権限範囲で指定されたデータにアクセスすることはできません。データにアクセスするには、被付与者は AWS CLI、アプリケーション、またはその他の AWS サービスを通じてアクセスする必要があります。

許可

☒ 読み込み

☒ 書き込み

被付与者タイプ [情報](#)

☒ IAM アイデンティティセンターからのディレクトリ ID

☐ IAM プリンシパル

ディレクトリアイデンティティタイプ [情報](#)

☒ ユーザー

☐ グループ

IAM アイデンティティセンターユーザー ID [情報](#)

このレベルのアクセスを許可したいユーザー。ID は IAM アイデンティティセンターコンソール [で確認](#) できます。

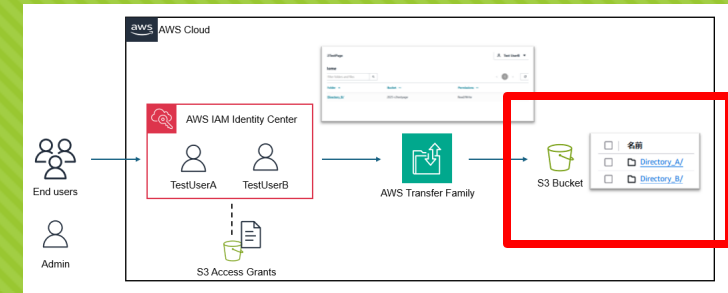
フォーマット: a1b2c3d4-e678-90ab-cdef-EXAMPLE11111

▶ アプリケーション - オプション

[キャンセル](#) [権限を作成](#)

ロケーション、IAMロールの登録。ユーザーとの紐づけも実施。

④ CORSの設定



Cross-Origin Resource Sharing (CORS) を編集 情報

Cross-Origin Resource Sharing (CORS)

JSON で記述された CORS 設定は、特定のドメインにロードされたクライアントウェブアプリケーションが異なるドメイン内のリソースと通信する方法を定義します。 [詳細はこちら](#)

```
1 [
2   {
3     "AllowedHeaders": [
4       ""
5     ],
6     "AllowedMethods": [
7       "GET",
8       "PUT",
9       "POST",
10      "DELETE",
11      "HEAD"
12    ],
13    "AllowedOrigins": [
14      "https://[redacted]"
15    ],
16    "ExposeHeaders": [
17      "last-modified",
18      "content-length",
19      "etag",
20      "x-amz-version-id",
21      "content-type",
22      "x-amz-request-id",
23      "x-amz-id-2",
24      "date"
25    ]
26  }
27 ]
```

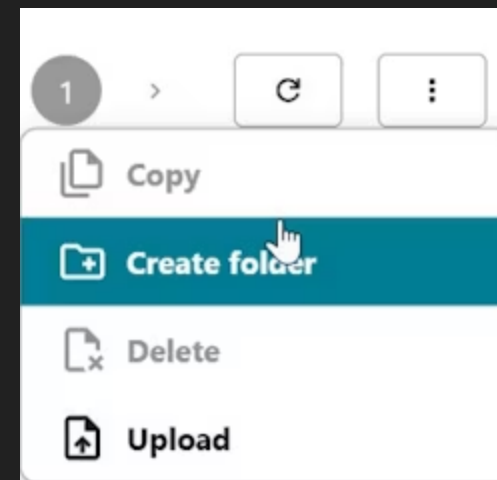
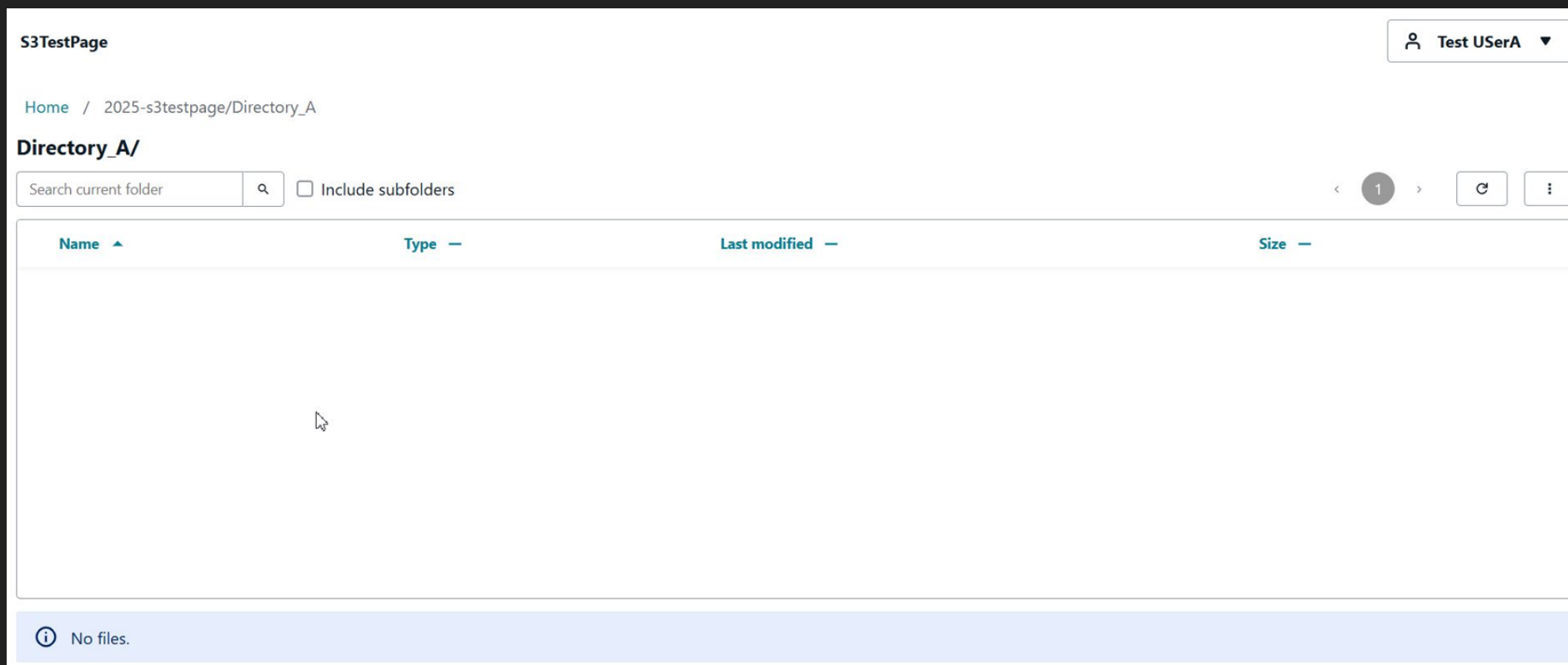
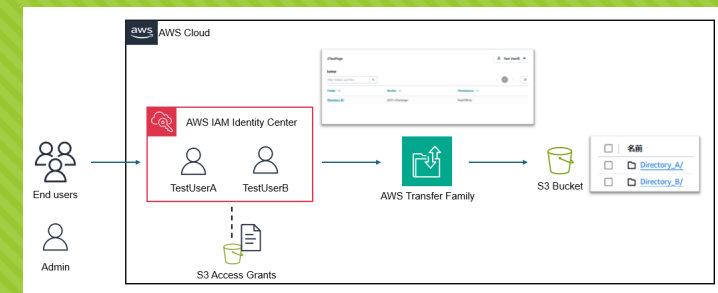
JSON Ln 14, Col 79 エラー: 0 | 警告: 0

キャンセル

変更の保存

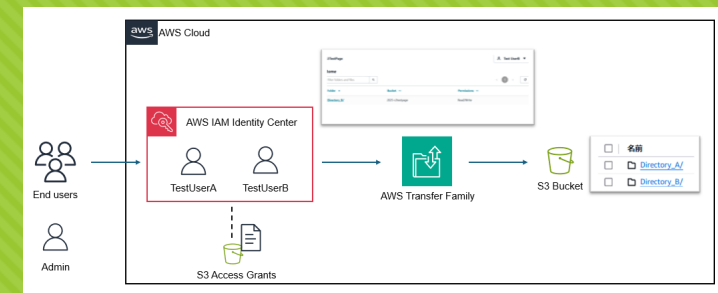
参照 : [Set up Cross-origin resource sharing \(CORS\) for your bucket - AWS Transfer Family](#)

⑤ アクセス・操作を実施



アプリケーションを見ることができた。様々な操作が可能。

⑤ アクセス・操作を実施



S3TestPage

Test UserA

Exit

Upload

Overwrite existing files

Add folder Add files

Name	Folder	Type	Size	Status	Progress
weblogo.jpg	-	jpg	212.8 kB	Completed	100%

Destination Directory_A

Completed 1/1 Failed 0/1 Canceled 0/1 Not started 0/1

All files uploaded.

Cancel Upload

Directory_A/

オブジェクト プロパティ

オブジェクト (1) 情報

オブジェクトは、Amazon S3 に保存された基本的なエンティティです。Amazon S3 インベントリを使用してアクセス権限を付与する必要があります。詳細はこちら

プレフィックスでオブジェクトを検索

名前	タイプ
weblogo.jpg	jpg

試しにアップロードを実施。S3バケット上でも確認できた。

まとめ

- 良かった点
 - セットアップはノーコードでお手軽にできる
 - 機能が比較的豊富で使いやすい
 - ファイルアップロード、削除、コピー（複数ファイル同時も可）、フォルダ作成、バケット内全検索
- その他感じたこと
 - IAM Identity Center、S3 Access Grants に慣れている必要がある
 - 従量課金制だが、高い…（USD0.50/時間/ユニット）
- 次回やってみたいこと
 - CloudFrontと組み合わせることでカスタムドメインに変更してみる
 - Storage Browser for Amazon S3を試してみる