aws

管理ガイド

Amazon WorkDocs

Amazon WorkDocs: 管理ガイド

Table of Contents

注意: 新しい顧客のサインアップとアカウントのアップグレードは、Amazon WorkDocs では利用できなくなりました。移行手順については、WorkDocs からデータを移行する方法」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。

Amazon WorkDocs とは何ですか？

Amazon WorkDocs は、フルマネージド型の安全なエンタープライズストレージおよび共有サービスであり、ユーザーの生産性を高める強力な管理制御とフィードバック機能を備えています。ファイルは、クラウド内に安全に保存されます。ユーザーのファイルは、ユーザーのみ、またはユーザーが指定したコントリビューターとビューワーのみが閲覧できます。ユーザーの組織のその他の方は、ユーザーが特別なアクセス許可を付与しない限り、ユーザーのいずれのファイルへもアクセスすることができません。

ユーザーはコラボレーション、または、レビューの目的で、その他の方とファイルを共用することができます。WorkDocs クライアントアプリケーションを使用して、ファイルのインターネットメディアタイプに応じて、さまざまなタイプのファイルを表示できます。WorkDocs はすべての一般的なドキュメントおよびイメージ形式をサポートし、追加のメディアタイプのサポートが常に追加されています。

詳細については、「Amazon WorkDocs」をご参照ください。

WorkDocs へのアクセス

管理者は WorkDocs コンソールを使用して WorkDocs サイトを作成および非アクティブ化します。管理コントロールパネルを使用して、ユーザー、ストレージ、およびセキュリティの設定を管理できます。詳細については、「サイト管理者コントロールパネルからの WorkDocs の管理」および「WorkDocs ユーザーの招待と管理」をご参照ください。

管理者以外のユーザーはクライアントアプリケーションを使用してファイルにアクセスします。WorkDocs コンソールや管理ダッシュボードは使用しません。WorkDocs には、いくつかの異なるクライアントアプリケーションとユーティリティが用意されています。

- ドキュメント管理とレビューに使用するウェブアプリケーション。
- ドキュメントレビューに使用するモバイルデバイス用ネイティブアプリケーション。
- WorkDocs Drive は、macOS または Windows デスクトップ上のフォルダを WorkDocs ファイルと同期させるアプリです。

ユーザーが WorkDocs クライアントをダウンロードし、ファイルを編集し、フォルダを使用する方法の詳細については、WorkDocs ユーザーガイド」の以下のトピックを参照してください。

- WorkDocs の開始方法

- ファイルの使用
- フォルダの操作

料金

WorkDocs では、前払い料金やコミットメントはありません。アクティブなユーザーアカウントと、使用するストレージに対する料金のみです。 詳細については、[料金]を参照してください。

開始方法

WorkDocs の使用を開始するには、「」を参照してくださいWorkDocs サイトの作成。

WorkDocs からのデータの移行

WorkDocs には、WorkDocs サイトからデータを移行するための 2 つの方法があります。このセクションでは、これらの方法の概要と、各移行方法を実行、トラブルシューティング、最適化するための詳細な手順へのリンクを提供します。

Amazon WorkDocs からデータをオフボードするには、既存の一括ダウンロード機能 (方法 1) または新しいデータ移行ツール (方法 2) の 2 つのオプションがあります。以下のトピックでは、両方の方法を使用する方法について説明します。

トピック

方法 1: ファイルを一括ダウンロードする

移行するファイルを制御したい場合は、手動で一括ダウンロードできます。この方法では、必要なファイルのみを選択し、ローカルドライブなどの別の場所にダウンロードできます。ファイルとフォルダは、WorkDocs ウェブサイトまたは WorkDocs Drive からダウンロードできます。

次の点に注意してください。

- サイトユーザーは、以下の手順に従ってファイルをダウンロードできます。必要に応じて、共有フォルダを設定し、ユーザーにファイルをそのフォルダに移動させ、フォルダを別の場所にダウンロードさせることができます。所有権を自分に移管し、ダウンロードを実行することもできます。
- コメントを含む Microsoft Word ドキュメントをダウンロードするには、「WorkDocs ユーザーガイド」の「フィードバックを含む Word ドキュメントのダウンロード」を参照してください。 WorkDocs
- 5 GB を超えるファイルをダウンロードするには、WorkDocs Drive を使用する必要があります。
- WorkDocs Drive を使用してファイルとフォルダをダウンロードする場合、ディレクトリ構造、ファイル名、ファイルコンテンツはそのまま残ります。ファイルの所有権、アクセス許可、バージョンは保持されません。

ウェブからのファイルのダウンロード

このメソッドを使用して、次の場合にファイルをダウンロードします。

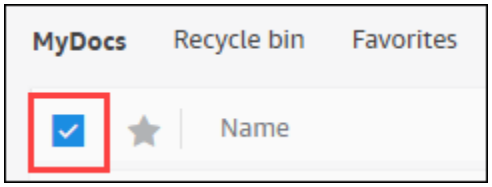
- 一部のファイルはサイトからのみダウンロードします。
- コメントを含む Word ドキュメントをダウンロードし、それらのコメントをそれぞれのドキュメントに保持します。移行ツールはすべてのコメントをダウンロードしますが、別の XML ファイルに書き込みます。その後、サイトユーザーはコメントと Word ドキュメントの関連付けに問題がある可能性があります。

ウェブからファイルをダウンロードするには

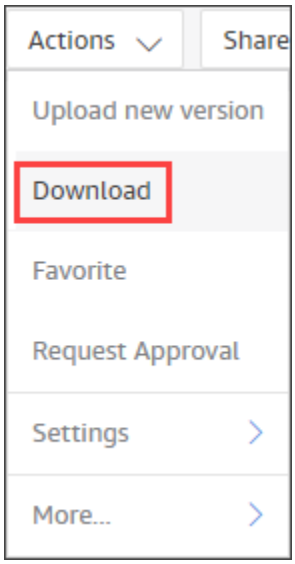
1. WorkDocs にサインインします。
2. 必要に応じて、ダウンロードするファイルを含むフォルダを開きます。
3. ダウンロードするファイルの横にあるチェックボックスをオンにします。

   —OR—

   リストの上部にあるチェックボックスをオンにして、フォルダ内のすべてのファイルを選択します。



4. Actions メニューを開き、Download を選択します。



PC では、ダウンロードされたファイルはデフォルトでDownloads/WorkDocsDownloads/フォルダ名に表示されます。Macintosh では、ファイルはデフォルトでハードドライブ名/Users/user name/WorkDocsDownloads になります。

ウェブからフォルダをダウンロードする

> **Note**
>
> フォルダをダウンロードするときは、フォルダ内のすべてのファイルもダウンロードします。フォルダ内のファイルの一部のみをダウンロードし、不要なファイルを別の場所に移動するか、ごみ箱に移動する場合は、フォルダをダウンロードします。

ウェブからフォルダをダウンロードするには

1. WorkDocs にサインインする
2. ダウンロードする各フォルダの横にあるチェックボックスをオンにします。

   —OR—

   フォルダを開き、ダウンロードするサブフォルダの横にあるチェックボックスをオンにします。
3. Actions メニューを開き、Download を選択します。

   PC では、ダウンロードされたフォルダーはデフォルトで Downloads/WorkDocsDownloads/フォルダー名に配置されます。Macintosh では、ファイルはデフォルトでハードドライブ名/Users/user name/WorkDocsDownloads になります。

WorkDocs Drive を使用してファイルとフォルダをダウンロードする

> **Note**
>
> 次の手順を完了するには、WorkDocs Drive をインストールする必要があります。詳細については、WorkDocs Drive ユーザーガイド」のWorkDocs Drive のインストール」を参照してください。

WorkDocs Drive からファイルとフォルダをダウンロードするには

1. File Explorer または Finder を起動し、W: ドライブを開きます。
2. ダウンロードするフォルダまたはファイルを選択します。
3. 選択した項目を長押し (右クリック) してコピーを選択し、コピーした項目を新しい場所に貼り付けます。

   —OR—

   選択した項目を新しい場所にドラッグします。
4. WorkDocs Drive から元のファイルを削除します。

方法 2: 移行ツールを使用する

WorkDocs サイトからすべてのデータを移行する場合は、WorkDocs 移行ツールを使用します。

移行ツールは、データをサイトから Amazon Simple Storage Service バケットに移動します。このツールは、ユーザーごとに圧縮された ZIP ファイルを作成します。zip ファイルには、WorkDocs サイトの各エンドユーザーのすべてのファイルとフォルダ、バージョン、アクセス許可、コメント、注釈が含まれます。

トピック

前提条件

移行ツールを使用するには、次の項目が必要です。

- Amazon S3 バケット。Amazon S3 バケットの作成の詳細については、「Amazon Amazon S3ユーザーガイド」の「バケットの作成」を参照してください。バケットは同じ IAM アカウントを使用し、WorkDocs サイトと同じリージョンに存在する必要があります。また、バケットへのパブリッ

クアクセスをブロックする必要があります。詳細については、Amazon S3 ユーザーガイド」の「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。 Amazon S3

ファイルをアップロードするアクセス許可を WorkDocs に付与するには、次の例に示すようにバケットポリシーを設定します。ポリシーは、 `aws:SourceAccount` および `aws:SourceArn`条件キーを使用してポリシーの範囲を狭めます。これは、セキュリティのベストプラクティスです。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowWorkDocsFileUpload",
            "Effect": "Allow",
            "Principal": {
                "Service": "workdocs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS-ACCOUNT-ID"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:workdocs:REGION:AWS-ACCOUNT-
ID:organization/WORKDOCS-DIRECTORY-ID"
                }
            }
        }
    ]
}
```

> **Note**
>
> - *WORKDOCS-DIRECTORY-ID* は、WorkDocs サイトの組織 ID です。これは、AWS WorkDocs コンソールの「My Sites」テーブルにあります。
> - バケットポリシーの設定の詳細については、Amazon S3コンソールを使用したバケットポリシーの追加」を参照してください。

- IAM ポリシー。WorkDocs コンソールで移行を開始するには、IAM 呼び出し元プリンシパルに、アクセス許可セットに次のポリシーがアタッチされている必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStartWorkDocsMigration",
            "Effect": "Allow",
            "Action": [
                "workdocs:StartInstanceExport"
            ],
            "Resource": [
                "arn:aws:workdocs:REGION:AWS-ACCOUNT-ID:organization/WORKDOCS-
DIRECTORY-ID"
            ]
        },
        {
            "Sid": "AllowDescribeWorkDocsMigrations",
            "Effect": "Allow",
            "Action": [
                "workdocs:DescribeInstanceExports",
                "workdocs:DescribeInstances"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AllowS3Validations",
            "Effect": "Allow",
            "Action": [
                "s3:HeadBucket",
                "s3:ListBucket",
                "s3:GetBucketPublicAccessBlock",
                "kms:ListAliases"
            ],
            "Resource": [
                "arn:aws:s3:::BUCKET-NAME"
            ]
        },
        {
            "Sid": "AllowS3ListMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
```

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- 必要に応じて、 AWS KMS キーを使用してバケット内の保管時のデータを暗号化できます。キーを指定しない場合、バケットの標準暗号化設定が適用されます。詳細については、「 Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。 AWS

  AWS KMS キーを使用するには、IAM ポリシーに次のステートメントを追加します。SYMMETRIC_DEFAULT タイプのアクティブなキーを使用する必要があります。

```
{
    "Sid": "AllowKMSMigration",
     "Effect": "Allow",
     "Action": [
         "kms:CreateGrant",
         "kms:DescribeKey"
     ],
     "Resource": [

         "arn:aws:kms:REGION:AWS-ACCOUNT-ID:key/KEY-RESOURCE-ID"
     ]
}
```

制限

移行ツールには以下の制限があります。

- このツールは、すべてのユーザーのアクセス許可、コメント、注釈を個別の CSV ファイルに書き込みます。そのデータを対応するファイルに手動でマッピングする必要があります。
- アクティブなサイトのみを移行できます。
- このツールは、24 時間ごとにサイトごとに 1 回の成功した移行に制限されています。
- 同じサイトの同時移行を実行することはできませんが、異なるサイトに対して同時移行を実行できます。

- 各 zip ファイルは最大 50GB になります。WorkDocs に 50GB を超えるデータがあるユーザーは、複数の zip ファイルを Amazon S3 にエクスポートします。
- このツールは 50 GB を超えるファイルをエクスポートしません。このツールは、ZIP ファイルと同じプレフィックスを持つ CSV ファイル内の 50 GB を超えるファイルを一覧表示します。たとえば、/workdocs/*site-alias*/*created-timestamp-UTC*/skippedFiles.csv です。リストされたファイルは、プログラムまたは手動でダウンロードできます。プログラムによるダウンロードの詳細については、https://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.htmlWorkDocs デベロッパーガイド」の「」を参照してください。ファイルを手動でダウンロードする方法については、このトピックの前半の「方法 1」の手順を参照してください。
- 各ユーザーの zip ファイルには、ユーザーが所有しているファイルやフォルダのみが含まれます。ユーザーと共有されているファイルやフォルダは、ファイルやフォルダを所有するユーザーの zip ファイルにあります。
- WorkDocs でフォルダが空の場合 (ネストされたファイル/フォルダが含まれていない場合) 、エクスポートされません。
- 移行ジョブの開始後に作成されたデータ (ファイル、フォルダ、バージョン、コメント、注釈) が S3 のエクスポートされたデータに含まれるとは限りません。
- 複数のサイトを Amazon S3 バケットに移行できます。サイトごとに 1 つのバケットを作成する必要はありません。ただし、IAM ポリシーとバケットポリシーで複数のサイトが許可されていることを確認する必要があります。
- 移行すると、バケットに移行するデータの量に応じて、Amazon S3 のコストが増加します。詳細については、Amazon S3 の料金ページを参照してください。

移行ツールの実行

次の手順では、WorkDocs 移行ツールを実行する方法について説明します。

サイトを移行するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. ナビゲーションペインで、マイサイトを選択し、移行するサイトの横にあるラジオボタンを選択します。
3. Actions リストを開き、Migrate Data を選択します。
4. 「Migrate Data site-name」ページで、Amazon S3 バケットの URI を入力します。

   —OR—

S3 を参照を選択し、以下の手順に従います。

a. 必要に応じて、バケットを検索します。

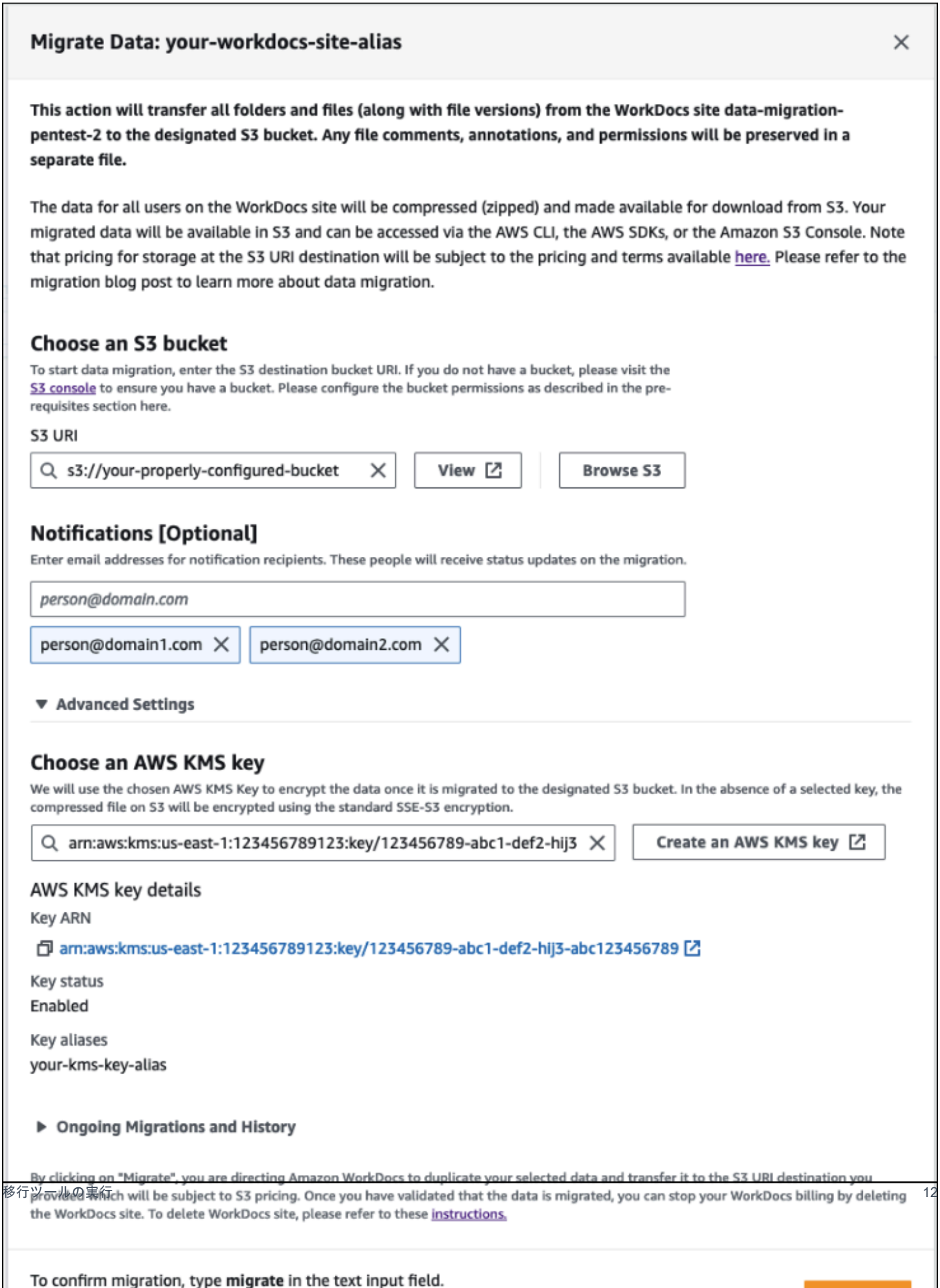
b. バケット名の横にあるラジオボタンを選択し、選択を選択します。

5. (オプション) 通知に、最大 5 つの E メールアドレスを入力します。このツールは、移行ステータスの E メールを各受信者に送信します。

6. (オプション) 詳細設定で、保存されたデータを暗号化する KMS キーを選択します。

7. テキストボックス**migrate**に「」と入力して移行を確認し、「移行の開始」を選択します。

インジケータが表示され、移行のステータスが表示されます。移行時間は、サイトのデータ量によって異なります。


Migrate Data: your-workdocs-site-alias
This action will transfer all folders and files (along with file versions) from the WorkDocs site data-migration-pentest-2 to the designated S3 bucket. Any file comments, annotations, and permissions will be preserved in a separate file.
The data for all users on the WorkDocs site will be compressed (zipped) and made available for download from S3. Your migrated data will be available in S3 and can be accessed via the AWS CLI, the AWS SDKs, or the Amazon S3 Console. Note that pricing for storage at the S3 URI destination will be subject to the pricing and terms available here. Please refer to the migration blog post to learn more about data migration.
Choose an S3 bucket
To start data migration, enter the S3 destination bucket URI. If you do not have a bucket, please visit the S3 console to ensure you have a bucket. Please configure the bucket permissions as described in the pre-requisites section here.
S3 URI
s3://your-properly-configured-bucket
View
Browse S3
Notifications [Optional]
Enter email addresses for notification recipients. These people will receive status updates on the migration.
person@domain.com
person@domain1.com
person@domain2.com
Advanced Settings
Choose an AWS KMS key
We will use the chosen AWS KMS Key to encrypt the data once it is migrated to the designated S3 bucket. In the absence of a selected key, the compressed file on S3 will be encrypted using the standard SSE-S3 encryption.
arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3
Create an AWS KMS key
AWS KMS key details
Key ARN
arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3-abc123456789
Key status
Enabled
Key aliases
your-kms-key-alias
Ongoing Migrations and History
By clicking on "Migrate", you are directing Amazon WorkDocs to duplicate your selected data and transfer it to the S3 URI destination you provided which will be subject to S3 pricing. Once you have validated that the data is migrated, you can stop your WorkDocs billing by deleting the WorkDocs site. To delete WorkDocs site, please refer to these instructions.
To confirm migration, type migrate in the text input field.

移行が終了すると、次のようになります。

- このツールは、セットアップ中に入力したアドレスに「成功」メールを送信します。
- Amazon S3 バケットには、/workdocs/*site-alias*/*created-timestamp-UTC*/ フォルダが含まれます。そのフォルダには、サイトにデータがある各ユーザーの zip フォルダが含まれています。各 zip フォルダには、アクセス許可とコメントマッピング CSV ファイルなど、ユーザーのフォルダとファイルが含まれています。
- 移行前にユーザーがすべてのファイルを削除した場合、そのユーザーの zip フォルダは表示されません。
- バージョン – 複数のバージョンを持つドキュメントには、_version_creation タイムスタンプ識別子があります。タイムスタンプはエポックミリ秒を使用します。たとえば、2 つのバージョンを持つTestFile.txt”」という名前のドキュメントは次のようになります。

```
        TestFile.txt (version 2 - latest version)
        TestFile_version_1707437230000.txt
```

- アクセス許可 – 次の例は、一般的なアクセス許可 CSV ファイルの内容を示しています。

```
PathToFile,PrincipalName,PrincipalType,Role
/mydocs/Projects,user1@domain.com,USER,VIEWER
/mydocs/Personal,user2@domain.com,USER,VIEWER
/mydocs/Documentation/Onboarding_Guide.xml,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Documentation/Onboarding_Guide.xml,user1@domain.com,USER,CONTRIBUTOR
/mydocs/Projects/Initiative,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Notes,user2@domain.com,USER,COOWNER
/mydocs/Notes,user1@domain.com,USER,COOWNER
/mydocs/Projects/Initiative/Structures.xml,user3@domain.com,USER,COOWNER
```

- コメント – 次の例は、一般的なコメント CSV ファイルの内容を示しています。

```
PathToFile,PrincipalName,PostedTimestamp,Text
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:57:40.781Z,TEST ANNOTATION 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:18:09.812Z,TEST ANNOTATION 2
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:20:04.099Z,TEST ANNOTATION 3
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:56:27.390Z,TEST COMMENT 1
```

```
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:17:10.348Z,TEST COMMENT 2
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:19:42.821Z,TEST COMMENT 3
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T22:21:09.930Z,TEST ANNOTATION 4
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T20:57:04.931Z,TEST COMMENT 4
```

- スキップされたファイル – 次の例は、一般的なスキップされたファイルの CSV ファイルの内容を示しています。ID を短縮し、読みやすくするために理由値をスキップしました。

```
FileOwner,PathToFile,DocumentId,VersionId,SkippedReason
user1@domain.com,/mydocs/LargeFile1.mp4,45e433b5469...,170899345...,The file is too
 large. Please notify the document owner...
user2@domain.com,/mydocs/LargeFile2.pdf,e87f725898c1...,170899696...,The file is too
 large. Please notify the document owner...
```

Amazon S3 から移行されたデータをダウンロードする

移行すると Amazon S3 のコストが増加するため、移行したデータを Amazon S3 から別のストレージソリューションにダウンロードできます。このトピックでは、移行したデータをダウンロードする方法について説明し、ストレージソリューションにデータをアップロードするための提案を提供します。

> **Note**
>
> 次の手順では、一度に 1 つのファイルまたはフォルダをダウンロードする方法について説明します。ファイルをダウンロードするその他の方法については、Amazon S3ユーザーガイド」の「オブジェクトのダウンロード」を参照してください。

データをダウンロードするには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ターゲットバケットを選択し、サイトエイリアスに移動します。
3. zip フォルダの横にあるチェックボックスをオンにします。

   —OR—

zip フォルダを開き、個々のユーザーのファイルまたはフォルダの横にあるチェックボックスをオンにします。

4. [ダウンロード] を選択します。

ストレージソリューションの提案

大規模なサイトでは、準拠の Linux ベースの Amazon マシンイメージを使用して EC2 インスタンスをプロビジョニングし、Amazon S3 からプログラムでデータをダウンロードし、データを解凍してから、ストレージプロバイダーまたはローカルディスクにアップロードすることをお勧めします。

移行のトラブルシューティング

以下のステップを試して、環境が正しく設定されていることを確認します。

- 移行が失敗すると、WorkDocs コンソールの移行履歴タブにエラーメッセージが表示されます。エラーメッセージを確認します。
- Amazon S3 バケットの設定を確認します。
- 移行を再実行します。

問題が解決しない場合は、AWS Support までお問い合わせください。移行履歴テーブルにある WorkDocs サイト URL と移行ジョブ ID を含めます。

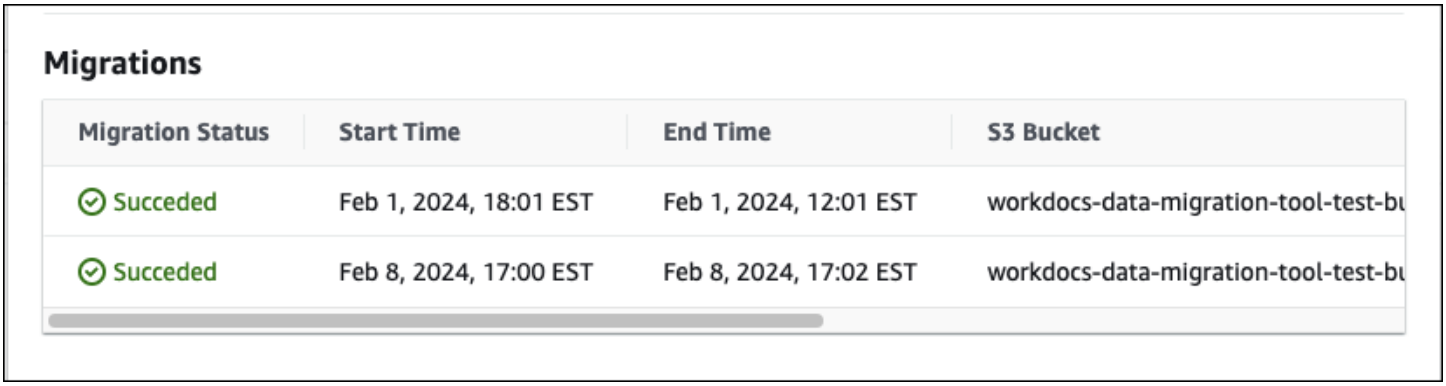
移行履歴の表示

次の手順では、移行履歴を表示する方法について説明します。

履歴を表示するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. 目的の WorkDocs サイトの横にあるラジオボタンを選択します。
3. Actions リストを開き、Migrate Data を選択します。
4. 「データサイト名の移行」ページで、「継続的な移行と履歴」を選択します。

移行履歴は移行の下に表示されます。次の図は、一般的な履歴を示しています。


Migrations
Migration Status
Start Time
End Time
S3 Bucket
Succeded
Feb 1, 2024, 18:01 EST
Feb 1, 2024, 12:01 EST
workdocs-data-migration-tool-test-bu
Succeded
Feb 8, 2024, 17:00 EST
Feb 8, 2024, 17:02 EST
workdocs-data-migration-tool-test-bu

Amazon WorkDocs の前提条件

新しい WorkDocs サイトをセットアップしたり、既存のサイトを管理したりするには、次のタスクを完了する必要があります。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一部では、電話またはテキストメッセージを受信し、電話のキーパッドに検証コードを入力します。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM アイデンティティセンター、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS マネジメントコンソールとして にサインインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「AWS IAM アイデンティティセンターの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、AWS IAM アイデンティティセンター 「 ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン 「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「グループの結合」を参照してください。

Amazon WorkDocs のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。「AWS 」 コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Amazon WorkDocs に適用されるコンプライアンスプログラムについて知るには、「コンプライアンスプログラムによるスコープ内のAWS サービス」を参照してください。
- クラウド内のセキュリティ – 使用する AWS サービスによって、お客様の責任が決まります。また、お客様は、 お客様のデータの機密性、企業の要件、および適用可能な法律や規制といった他の要因 についても責任を担います。このセクションのトピックは、WorkDocs を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。

> **Note**
>
> WorkDocs 組織のユーザーは、ファイルへのリンクまたは招待を送信することで、組織外のユーザーとコラボレーションできます。ただし、これは Active Directory Connector を使用するサイトにのみ適用されます。サイトの共有リンク設定を参照して、会社の要件に最も適したオプションを選択します。

以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように WorkDocs を設定する方法について説明します。また、WorkDocs リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- Amazon WorkDocs のアイデンティティおよびアクセス管理
- Amazon WorkDocs のロギングとモニタリング
- Amazon WorkDocs のコンプライアンスの検証

- Amazon WorkDocs の耐障害性
- Amazon WorkDocs のインフラストラクチャのセキュリティ

Amazon WorkDocs のアイデンティティおよびアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に WorkDocs リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon WorkDocs と IAM との連携方法
- Amazon WorkDocs ID ベースのポリシーの例
- Amazon WorkDocs ID とアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の使用方法は、WorkDocs で行う作業によって異なります。

サービスユーザー – WorkDocs サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの WorkDocs 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。WorkDocs の機能にアクセスできない場合は、「」を参照してくださいAmazon WorkDocs ID とアクセスのトラブルシューティング。

サービス管理者 – 社内の WorkDocs リソースを担当している場合は、通常、WorkDocs へのフルアクセスがあります。サービスユーザーがどの WorkDocs 機能とリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社が WorkDocs で IAM を使用する方法の詳細については、「」を参照してくださいAmazon WorkDocs と IAM との連携方法。

IAM 管理者 – IAM 管理者は、WorkDocs へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる WorkDocs アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkDocs ID ベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM アイデンティティセンター （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS マネジメントコンソール または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、 AWS サインイン ユーザーガイドの「 へのサインイン方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的

な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS マネジメントコンソール、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM アイデンティティセンター User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサー

ビス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS マネジメントコンソール、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所

有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

> **Note**
>
> WorkDocs は Slack Organizations のサービスコントロールポリシーをサポートしていません。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

Amazon WorkDocs と IAM との連携方法

IAM を使用して WorkDocs へのアクセスを管理する前に、WorkDocs で使用できる IAM 機能を理解しておく必要があります。WorkDocs およびその他の AWS のサービスが IAM と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

トピック

- WorkDocs アイデンティティベースのポリシー
- WorkDocs リソースベースのポリシー
- WorkDocs タグに基づく認可
- WorkDocs IAM ロール

WorkDocs アイデンティティベースのポリシー

IAM アイデンティティベースのポリシーでは、許可されるアクションまたは拒否されるアクションを指定できます。WorkDocs は特定のアクションをサポートしています。JSON ポリシーで使用する要素については、「IAM ユーザーガイド」 の「IAM JSON ポリシー要素のリファレンス」(IAM JSON) をご参照ください。

アクション

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

WorkDocs のポリシーアクションは、アクションの前にプレフィックス を使用しますworkdocs:。たとえば、WorkDocs `DescribeUsers` API オペレーションを実行するアクセス許可を付与するには、ポリシーに `workdocs:DescribeUsers`アクションを含めます。ポリシーステートメントに

はAction または NotAction 要素を含める必要があります。WorkDocs は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一のステートメントに複数のアクションを指定するには次のようにコンマで区切ります。

```
"Action": [
      "workdocs:DescribeUsers",
      "workdocs:CreateUser"
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Describe という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "workdocs:Describe*"
```

> **Note**
>
> 下位互換性を確保するには、 zocalo アクションを含めます。例えば:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

WorkDocs アクションのリストを確認するには、IAM ユーザーガイドのWorkDocs で定義されるアクション」を参照してください。

リソース

WorkDocs は、ポリシーでのリソース ARNs の指定をサポートしていません。

条件キー

WorkDocs はサービス固有の条件キーを提供しませんが、一部のグローバル条件キーの使用をサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

例

WorkDocs アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkDocs ID ベースのポリシーの例。

WorkDocs リソースベースのポリシー

WorkDocs はリソースベースのポリシーをサポートしていません。

WorkDocs タグに基づく認可

WorkDocs は、リソースのタグ付けやタグに基づくアクセスの制御をサポートしていません。

WorkDocs IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

WorkDocs での一時的な認証情報の使用

フェデレーションでサインインしたり、IAM ロールを引き受けたり、クロスアカウント ロールを引き受けたりするには、一時的な認証情報を使用することを強くお勧めします。一時的なセキュリティ認証情報を取得するには、AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

WorkDocs は一時的な認証情報の使用をサポートしています。

サービスにリンクされた役割

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

WorkDocs は、サービスにリンクされたロールをサポートしていません。

サービス役割

この機能により、ユーザーに代わってサービスがサービス役割を引き受けることが許可されます。この役割により、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービス役割はIAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者はこの役割の権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

WorkDocs はサービスロールをサポートしていません。

Amazon WorkDocs ID ベースのポリシーの例

> **Note**
>
> セキュリティを強化するために、可能な限り IAM ユーザーではなくフェデレーティッドユーザーを作成してください。

デフォルトでは、IAM ユーザーとロールには WorkDocs リソースを作成または変更するアクセス許可はありません。また、 AWS マネジメントコンソール、 AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

> **Note**
>
> 下位互換性を確保するため、ポリシーに `zocalo` アクションを含めます。例えば:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
            "zocalo:*",
            "workdocs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

これらの JSON ポリシードキュメント例を使用して IAM の ID ベースのポリシーを作成する方法については、「IAM User Guide」(IAM ユーザーガイド) の「Creating policies on the JSON tab」(JSON タブでのポリシーの作成) をご参照ください。

トピック

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが WorkDocs リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサ

ポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

WorkDocs コンソールの使用

Amazon WorkDocs コンソールにアクセスするには、最小限の権限のセットが必要です。これらのアクセス許可により、 AWS アカウントの WorkDocs リソースの詳細を一覧表示および表示できます。最小限必要な権限よりも制限の厳しい ID ベースのポリシーを作成すると、コンソールは IAM ユーザーまたはロールエンティティに対して意図されたとおりに機能しなくなります。

これらのエンティティが WorkDocs コンソールを使用できるようにするには、次の AWS 管理ポリシーもエンティティにアタッチします。IAM ポリシーをアタッチすることの詳細は、「IAM User Guide」(IAM ユーザーガイド) の「Adding permissions to a user」(IAM ユーザーのアクセス許可の追加) を参照してください。

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- AmazonEC2FullAccess

これらのポリシーは、WorkDocs リソース、 AWS Directory Service オペレーション、および Amazon WorkDocs が正しく動作するために必要な Amazon EC2 オペレーションへのフルアクセスをユーザーに付与します。 Amazon WorkDocs

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、

または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkDocs リソースへの読み取り専用アクセスをユーザーに許可する

次の AWS マネージド AmazonWorkDocsReadOnlyAccess ポリシーは、IAM ユーザーに WorkDocs リソースへの読み取り専用アクセスを許可します。このポリシーは、すべての WorkDocs `Describe`オペレーションへのアクセス権をユーザーに付与します。WorkDocs が VPCsとサブネットのリストを取得できるように、2 つの Amazon EC2 オペレーションにアクセスする必要

があります。 Directory Service ディレクトリに関する情報を取得するには、 Directory Service `DescribeDirectories`オペレーションへのアクセスが必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workdocs:Describe*",
                "ds:DescribeDirectories",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

その他の WorkDocs アイデンティティベースのポリシーの例

IAM 管理者は、IAM ロールまたはユーザーに WorkDocs API へのアクセスを許可する追加のポリシーを作成できます。詳細については、WorkDocs デベロッパーガイド」の「管理アプリケーションの認証とアクセスコントロール」を参照してください。

Amazon WorkDocs ID とアクセスのトラブルシューティング

以下の情報は、WorkDocs と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- WorkDocs でアクションを実行する権限がありません
- iam:PassRole を実行する権限がありません
- AWS アカウント以外のユーザーに WorkDocs リソースへのアクセスを許可したい

WorkDocs でアクションを実行する権限がありません

にアクションを実行する権限がないと AWS マネジメントコンソール 通知された場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

iam:PassRole を実行する権限がありません

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して WorkDocs にロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 という IAM ユーザーがコンソールを使用して WorkDocs `marymajor` でアクションを実行しようとすると発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

AWS アカウント以外のユーザーに WorkDocs リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- WorkDocs がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいAmazon WorkDocs と IAM との連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。

- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

Amazon WorkDocs のロギングとモニタリング

Amazon WorkDocs のサイト管理者は、サイト全体向けのアクティビティフィードを表示およびエクスポートすることができます。また、 を使用して AWS CloudTrail WorkDocs コンソールからイベントをキャプチャすることもできます。

トピック

- サイト全体のアクティビティフィードのエクスポート
- AWS CloudTrail を使用して Amazon WorkDocs API コールを口グに記録する

サイト全体のアクティビティフィードのエクスポート

管理者は、サイト全体のアクティビティフィードを表示、エクスポートすることができます。この機能を使用するには、まず WorkDocs Companion をインストールする必要があります。WorkDocs Companion をインストールするには、WorkDocs のアプリケーションと統合」を参照してください。

サイト全体のアクティビティフィードを表示、エクスポートするには

1. ウェブアプリケーションで、[Activity] (アクティビティ) を選択します。
2. [Filter](フィルター) を選択し、[Site-wide activity] (サイト全体のアクティビティ) スライダーを動かしてフィルターをオンにします。
3. [Activity Type] (アクティビティタイプ) フィルターを選択し、必要に応じて [Date Modified] (変更日) 設定を選択してから、[Apply] (適用) を選択します。
4. フィルタリングされたアクティビティフィードの結果が表示されたら、ファイル、フォルダ、またはユーザー名で検索して結果を絞り込みます。必要に応じてフィルタを追加または削除することも可能です。

5. [Export] (エクスポート) を選択して、アクティビティフィードをデスクトップ上の `.csv` および `.json` ファイルにエクスポートします。システムは、以下のいずれかの場所にファイルをエクスポートします。

   - [Windows] (ウインドウズ) – PC の [Downloads] (ダウンロード) フォルダ内の [WorkDocsDownloads] (WorkDocs をダウンロード) フォルダ
   - macOS – `/users/username/WorkDocsDownloads/folder`

   エクスポートされたファイルには、適用したすべてのフィルタが反映されます。

   > **Note**
   >
   > 管理者ではないユーザーは、自分のコンテンツのみのアクティビティフィードを表示およびエクスポートできます。詳細は、「Amazon WorkDocs ユーザーガイド」の「アクティビティフィードの表示」を参照してください。

AWS CloudTrail を使用して Amazon WorkDocs API コールをログに記録する

を使用して AWS CloudTrail、Amazon WorkDocs API コールをログに記録できます。CloudTrail は、WorkDocs でユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail はWorkDocs コンソールからの呼び出しや WorkDocs API へのコード呼び出しを含むWorkDocs のすべての APIs。

証跡を作成する場合は、WorkDocs のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を作成しない場合でも、CloudTrail コンソールのイベント履歴で最新のイベントを表示することはできます。

CloudTrail が収集する情報には、リクエスト、リクエストが行われた IP アドレス、リクエストを行ったユーザー、リクエストの日付が含まれます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail の WorkDocs 情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。WorkDocs でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに

CloudTrail イベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「CloudTrail Event 履歴でのイベントの表示」を参照してください。

WorkDocs のイベントなど、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、ログファイルを CloudTrail で Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべてのリージョンに適用されます。証跡は、AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- CloudTrail ログファイルを複数のリージョンから受け取る、複数のアカウントから CloudTrail ログファイルを受け取る

すべての WorkDocs アクションは CloudTrail によってログに記録され、Amazon WorkDocs API リファレンスに記載されています。例えば、`CreateFolder`、`DeactivateUser`、および `UpdateDocument` セクションを呼び出すと、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

WorkDocs ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リク

エストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、公開 API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

WorkDocs は、コントロールプレーンからのエントリとデータプレーンからのエントリの異なるタイプの CloudTrail エントリを生成します。2 つの重要な違いは、コントロールプレーンのユーザー ID が IAM ユーザーであることです。データプレーンエントリのユーザー ID は WorkDocs ディレクトリユーザーです。

> **Note**
>
> セキュリティを強化するために、可能な限り IAM ユーザーではなくフェデレーティッドユーザーを作成してください。

パスワード、認証トークン、ファイルコメント、ファイルコンテンツなどの機密情報は、ログエントリには表示されません。これらは CloudTrail ログに HIDDEN_DUE_TO_SECURITY_REASONS として表示されます。これらは CloudTrail ログに HIDDEN_DUE_TO_SECURITY_REASONS として表示されます。

次の例は、WorkDocs の 2 つの CloudTrail ログエントリを示しています。最初のレコードはコントロールプレーンアクション用、2 つ目はデータプレーンアクション用です。

```
{
  Records : [
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "user_id",
        "arn" : "user_arn",
        "accountId" : "account_id",
        "accessKeyId" : "access_key_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "eventName" : "RemoveUserFromGroup",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
```

```
      "requestParameters" :
      {
        "directoryId" : "directory_id",
        "userSid" : "user_sid",
        "group" : "group"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    },
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "Unknown",
        "principalId" : "user_id",
        "accountId" : "account_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "AuthenticationToken" : "**-redacted-**"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    }
  ]
}
```

Amazon WorkDocs のコンプライアンスの検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス「コンプライアンスプログラムによる対象範囲内」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべての AWS のサービス が HIPAA の対象となるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub CSPM – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 不審なアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで AWS アカウント、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon WorkDocs の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「グローバルインフラストラクチャ」を参照してください。

Amazon WorkDocs のインフラストラクチャのセキュリティ

マネージドサービスである Amazon WorkDocs は、 AWS グローバルネットワークセキュリティ手順で保護されています。詳細については、IAM ユーザーガイドのAWS Identity and Access Management のインフラストラクチャセキュリティ」および AWS アーキテクチャセンターの「セキュリティ、アイデンティティ、コンプライアンスのベストプラクティス」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で WorkDocs にアクセスします。クライアントで Transport Layer Security (TLS) 1.2 がサポートされている必要があります。クライアントは、Ephemeral Diffie-Hellman や Elliptic Curve Ephemeral Diffie-Hellman などの完全転送秘密を備えた暗号スイートもサポートする必要があります。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token ServiceAWS STSを使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

WorkDocs の開始方法

WorkDocs はディレクトリを使用して、ユーザーとそのドキュメントの組織情報を保存および管理します。次に、サイトをプロビジョニングする際には、ディレクトリをサイトにアタッチします。これを行うと、自動アクティベーションと呼ばれる WorkDocs 機能によって、ディレクトリ内のユーザーがマネージドユーザーとしてサイトに追加されます。つまり、ユーザーはサイトにログインするために個別の認証情報を必要とせず、ファイルを共有して共同作業できます。追加購入しない限り、各ユーザーには 1 TB のストレージがあります。

ユーザーの追加やアクティベーションを手動で行う必要がなくなったとはいえ、まだ可能です。また必要に応じて、いつでもユーザーのロールおよび権限を変更することもできます。それを行うことについての詳細は、本ガイドで後述する「WorkDocs ユーザーの招待と管理」を参照してください。

ディレクトリを作成する必要がある場合は、以下のことができます。

- Simple AD ディレクトリを作成します。
- AD Connector ディレクトリを作成して、オンプレミス ディレクトリに接続します。
- WorkDocs が既存の AWS ディレクトリと連携できるようにします。
- WorkDocs にディレクトリを作成してもらいます。

AD ディレクトリと AWS Managed Microsoft AD ディレクトリの間に信頼関係を作成することもできます。

> **Note**
>
> PCI、 FedRAMP または DoD などのコンプライアンス プログラムに属している場合は、コンプライアンス要件を満たすために AWS Managed Microsoft AD ディレクトリを設定する必要があります。このセクションのステップでは、既存の Microsoft AD Directory の使用方法について説明します。Microsoft AD ディレクトリの作成の詳細については、「AWS Directory Service Administration Guide」 の「AWS Managed Microsoft AD」を参照してください。

内容

- 多要素認証の有効化
- ユーザーを管理者に昇格させる

WorkDocs サイトの作成

以下のセクションのステップでは、新しい WorkDocs サイトを設定する方法について説明します。

タスク

- [開始する前に]
- WorkDocs サイトの作成

[開始する前に]

WorkDocs サイトを作成する前に、次の項目が必要です。

- WorkDocs サイトを作成および管理するための AWS アカウント。ただし、ユーザーは WorkDocs に接続して使用するために AWS アカウントを必要としません。詳細については、「Amazon WorkDocs の前提条件」を参照してください。
- Simple AD を使用する予定がある場合は、「AWS Directory Service CC 管理ガイド」の「Simple AD の前提条件」に記載されている前提条件を満たす必要があります。
- PCI、FedRAMP、DoD などのコンプライアンスプログラムに属 AWS Managed Microsoft AD している場合は ディレクトリ。このセクションのステップでは、既存の Microsoft AD Directory の使用方法について説明します。Microsoft AD ディレクトリの作成の詳細については、「AWS Directory Service Administration Guide」の「AWS Managed Microsoft AD」を参照してください。
- 管理者のプロフィール情報 (姓名、電子メールアドレスなど)

WorkDocs サイトの作成

WorkDocs サイトを数分で作成するには、次の手順に従います。

WorkDocs サイトを作成するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. コンソールのホームページの [WorkDocs サイトを作成] で、[今すぐ開始] を選択します。

   —OR—

ナビゲーションペインで [マイサイト] を選択し、[WorkDocs サイトの管理] ページで [WorkDocs サイトを作成] を選択します。

次に実行される処理は、ディレクトリがあるかどうかによって異なります。

- ディレクトリがある場合は、「ディレクトリを選択」ページが表示され、既存のディレクトリを選択するか、ディレクトリを作成できます。
- ディレクトリがない場合は、「ディレクトリタイプを設定」ページが表示され、Simple AD または AD Connector ディレクトリを作成できます。

このステップでは、両方のタスクを実行する方法を説明します。

既存のディレクトリを使用するには

1. 使用可能なディレクトリリストを開き、使用するディレクトリを選択します。
2. [Enable directory] (ディレクトリディレクトリの有効化) を選択します。

ディレクトリを作成するには

1. 上記ステップ 1 と 2 を繰り返します。

   この時点で、Simple AD を使用するか AD Connector を作成するかによって、実行する内容が異なります。

   Simple ADを使用するには

   a. [Simple AD] を選択して、次に [次へ] を選択します。

      「Simple AD サイトを作成」ページが表示されます。

   b. 「アクセスポイント」の「サイト URL」ボックスに、サイトの URL を入力します。

   c. 「WorkDocs 管理者を設定」で、管理者のメールアドレス、名、姓を入力します。

   d. 必要に応じて、[ディレクトリの詳細] と [VPC 設定] のオプションを入力します。

   e. [Simple ADを作成] を選択します。

AD Connector ディレクトリを作成するには

a. [AD Connector]、 [次へ]の順に選択します。

[AD Connector のサイトを作成] ページが表示されます。

b. [ディレクトリの詳細] のすべてのフィールドに入力します。

c. [アクセスポイント] の [サイト URL] ボックスに、サイトの URL を入力します。

d. 必要に応じて、VPC 設定の下のオプションフィールドを入力します。

e. [AD Connector のサイトを作成] を選択します。

WorkDocs は以下を実行します。

- 上記のステップ 4 でユーザーに代わって VPC を設定するを選択した場合、WorkDocs はユーザーに代わって VPC を作成します。VPC のディレクトリには、ユーザーと WorkDocs サイト情報が保存されます。
- Simple AD を使用した場合、WorkDocs はディレクトリユーザーを作成し、そのユーザーを WorkDocs 管理者として設定します。AD Connector ディレクトリを作成した場合、WorkDocs は WorkDocs 管理者として指定した既存のディレクトリユーザーを設定します。
- 既存のディレクトリを使用した場合、WorkDocs は WorkDocs 管理者のユーザー名を入力するように求めます。ユーザーは、ディレクトリのメンバーでなければなりません。

> **Note**
>
> WorkDocs は、新しいサイトについてユーザーに通知しません。URL をユーザーに伝え、サイトを使用するために別のログインは必要がないことを知らせる必要があります。

シングルサインオンの有効化

AWS Directory Service では、ユーザーは、Amazon WorkDocsから Amazon WorkDocs にアクセスできます。認証情報を個別に入力する必要はありません。WorkDocs 管理者は、 Directory Service コンソールを使用してシングルサインオンを有効にできます。詳細については、「AWS Directory Service Administration Guide」(管理ガイド) の 「Single sign-on」(シングルサインオン) を参照してください。

WorkDocs 管理者がシングルサインオンを有効にした後、WorkDocs サイトユーザーは、シングルサインオンを許可するようにウェブブラウザ設定を変更する必要が生じる場合があります。詳細については、「AWS Directory Service 管理ガイド」の「Single sign-on for IE and Chrome」(IE および Chrome のシングルサインオン) および「Single sign-on for Firefox」(Firefox のシングルサインオン) を参照してください。

多要素認証の有効化

https://console.aws.amazon.com/directoryservicev2/ の AWS Directory Services Console を使用して、AD Connector ディレクトリの多要素認証を有効にします。MFA を有効にするには、MFA ソリューションとして Remote Authentication Dial-In User Service (RADIUS) サーバーを使用するか、オンプレミスインフラストラクチャに RADIUS サーバー用の MFA プラグインを実装しておく必要があります。MFA ソリューションでは、ワンタイムパスコード (OTP) を実装する必要があります。ユーザーは、ハードウェアデバイスから、または携帯電話などのデバイスで実行されるソフトウェアから、このコードを取得します、

RADIUS は、業界標準のクライアント/サーバープロトコルであり、ユーザーをネットワークサービスに接続するための認証、認可、アカウント管理の機能を提供します。AWS Managed Microsoft AD には、MFA ソリューションを実装した RADIUS サーバーに接続する RADIUS クライアントが付属しています。この RADIUS サーバーが、ユーザーネームと OTP コードを検証します。RADIUS サーバーがユーザーの検証に成功すると、 AWS Managed Microsoft AD は AD に対して、そのユーザーを認証します。AD に対する認証に成功すると、ユーザーは AWS アプリケーションにアクセスできます。Managed Microsoft AD RADIUS クライアントと RADIUS サーバーとの間の通信では、ポート 1812 を介した通信を有効にするための AWS セキュリティグループを設定する必要があります。

詳細については、AWS Directory Service 管理ガイドの「AWS Managed Microsoft AD の多要素認証を有効にする」を参照してください。

> **Note**
>
> Simple AD ディレクトリに対して多要素認証は使用できません。

ユーザーを管理者に昇格させる

WorkDocs コンソールを使用して、ユーザーを管理者に昇格させます。以下の手順に従ってください。

ユーザーを管理者に昇格するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. ナビゲーションペインで、[マイサイト] を選択します。

   WorkDocs サイトの管理ページが表示されます。
3. 目的のサイトの横にあるボタンを選択し、[アクション] を選択し、[管理者を設定] を選択します。

   WorkDocs 管理者を設定 ダイアログボックスが表示されます。
4. [ユーザー名] ボックスに、昇格させたいユーザーの名前を入力し、「管理者を設定」を選択します。

WorkDocs サイト管理者コントロールパネルを使用して、管理者を降格することもできます。詳細については、「ユーザーの編集」を参照してください。

AWS コンソールからの WorkDocs の管理

WorkDocs サイトを管理するには、以下のツールを使用します。

- AWS コンソールは https://console.aws.amazon.com/zocalo/ にあります。
- サイト管理者コントロールパネル。すべての WorkDocs サイトの管理者が使用できます。

これらのツールはそれぞれ異なる一連のアクションを提供し、このセクションのトピックでは、AWS コンソールによって提供されるアクションについて説明します。サイト管理コントロールパネルについては、「サイト管理者コントロールパネルからの WorkDocs の管理」を参照してください。

サイト管理者を設定する

管理者の場合は、サイトコントロールパネルとそこに表示されるアクションへのアクセスをユーザーに許可できます。

管理者を設定するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. ナビゲーションペインで、[マイサイト] を選択します。

   WorkDocs サイトの管理ページが表示され、サイトのリストが表示されます。
3. 管理者を設定するサイトの横にあるボタンを選択します。
4. [アクション] リストを開き、一覧から [管理者を設定] を選択します。

   WorkDocs 管理者を設定ダイアログボックスが表示されます。
5. 「ユーザー名」ボックスに新しい管理者の名前を入力し、「管理者を設定」を選択します。

招待メールの再送信

招待メールはいつでも再送信できます。

招待メールを再送信するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。

2. ナビゲーションペインで、[マイサイト] を選択します。

   WorkDocs サイトの管理ページが表示され、サイトのリストが表示されます。
3. メールを再送信するサイトの横にあるボタンを選択します。
4. 「アクション」リストを開き、「招待メールを再送信」を選択します。

   ページの上部に緑色のバナーで成功メッセージが表示されます。

多要素認証を管理する

WorkDocs サイトを作成した後、多要素認証を有効にできます。認証の詳細については、「多要素認証の有効化」を参照してください。

サイト間 URL の設定

> **Note**
>
> WorkDocs の開始方法でサイト作成プロセスを実行した場合は、サイト URL を入力したことになります。その結果、URL は 1 回しか設定できないため、WorkDocs ではサイト URL の設定コマンドを使用できません。Amazon WorkSpaces をデプロイして WorkDocs と統合する場合にのみ、これらのステップに従います。Amazon WorkSpaces の統合プロセスでは、サイト URL の代わりにシリアル番号を入力する必要があるため、統合を完了したら URL を入力する必要があります。Amazon WorkSpaces と WorkDocs の統合の詳細については、「Amazon WorkDocs との統合」を参照してください。 Amazon WorkSpaces

サイト URL を設定するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. ナビゲーションペインで、[マイサイト] を選択します。

   WorkDocs サイトの管理ページが表示され、サイトのリストが表示されます。
3. Amazon WorkSpaces と統合したサイトを選択します。URL には、https://{directory_id}.awsapps.com などの Amazon WorkSpaces インスタンスのディレクトリ ID が含まれています。
4. その URL の横にあるボタンを選択し、アクションリストを開いて [サイト URL を設定] を選択します。

「サイト URL を設定」ダイアログボックスが表示されます。

5. 「サイト URL」ボックスに、サイトの URL を入力し、「サイト URL を設定」を選択します。
6. [WorkDocs サイトの管理] ページで、[更新] を選択して新しい URL を表示します。

通知の管理

> **Note**
>
> セキュリティを強化するために、可能な限り IAM ユーザーではなくフェデレーティッドユーザーを作成してください。

通知により、IAM ユーザーまたはロールは CreateNotificationSubscription API を呼び出すことができます。これを使用して、WorkDocs が送信する SNS メッセージを処理するための独自のエンドポイントを設定できます。通知の詳細については、WorkDocs デベロッパーガイド」の「IAM ユーザーまたはロールの通知の設定」を参照してください。

通知の作成と削除が可能で、以下の手順でその方法を説明します。

> **Note**
>
> 通知を作成するには、IAM またはロール ARN が必要です。IAM ARN を検索するには、以下を実行します。
>
> 1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
> 2. ナビゲーションバーで、ユーザーを選択します。
> 3. ユーザー名を選択します。
> 4. 概要 で、ARN をコピーします。

通知を作成するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. ナビゲーションペインで、[マイサイト] を選択します。

   WorkDocs サイトの管理ページが表示され、サイトのリストが表示されます。

3. 目的のサイトの横にあるボタンを選択します。
4. 「アクション」リストを開き、「通知を管理」を選択します。

   通知の管理ページが表示されます。
5. [通知を作成] を選択します。
6. 新しい通知ダイアログボックスで、IAM またはロール ARN を入力し、通知の作成を選択します。

通知を削除するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. ナビゲーションペインで、[マイサイト] を選択します。

   WorkDocs サイトの管理ページが表示され、サイトのリストが表示されます。
3. 削除する通知があるサイトの横にあるボタンを選択します。
4. 「アクション」リストを開き、「通知を管理」を選択します。
5. 通知の管理ページで、削除する通知の横にあるボタンを選択し、通知の削除を選択します。

サイトの削除

WorkDocs コンソールを使用してサイトを削除します。

> **Warning**
>
> サイトを削除するとすべてのファイルが失われます。サイトを削除するのは、サイトのこの情報がもう必要ないと確信が持てる場合のみにしてください。

サイトを削除するには

1. https://console.aws.amazon.com/zocalo/ で WorkDocs コンソールを開きます。
2. ナビゲーションペインで、[マイサイト] を選択します。

   [WorkDocs サイトの管理] ページが表示されます。
3. 削除するルールの横にある [削除] ボタンを選択します。

[サイトURL]を[削除] ダイアログボックスが表示されます。

4. オプションで、[ユーザーディレクトリも削除する] を選択します。

> **Important**
>
> WorkDocs に独自のディレクトリを指定しない場合、自動的にディレクトリが作成されます。WorkDocs サイトを削除すると、そのディレクトリを削除するか、別の AWS アプリケーションに使用しない限り、作成したディレクトリに対して課金されます。料金情報については、「AWS Directory Service の料金」を参照してください。

5. 「サイトのURL」ボックスに、サイトのURL を入力し、[削除]を選択します。

サイトはすぐに削除され、使用できなくなります。

サイト管理者コントロールパネルからの WorkDocs の管理

WorkDocs サイトを管理するには、以下のツールを使用します。

- サイト管理者コントロールパネル。すべての WorkDocs サイトの管理者が使用でき、以下のトピックで説明します。
- AWS コンソールは https://console.aws.amazon.com/zocalo/ にあります。

これらのツールはそれぞれ異なるアクションセットを提供します。このセクションのトピックでは、サイト管理コントロールパネルが提供するアクションについて説明します。コンソールで利用できるタスクについては、「AWS コンソールからの WorkDocs の管理」を参照してください。

優先言語設定

E メール通知の言語を指定できます。

言語の設定を変更するには

1. [マイアカウント] で、[管理コントロールパネルを開く] を選択します。
2. [希望する言語の設定] で、希望する言語を選択します。

Hancom オンライン編集 と Office Online

[Admin control panel] (管理コントロールパネル) から、[Hancom Online Editing] (ハンコムオンライン編集) および [Office Online] (Office オンライン) の設定を有効または無効にします。詳細については、「共同編集の有効化」を参照してください。

[ストレージ]

新規ユーザーが受信するストレージの容量を指定します。

ストレージの設定を変更するには

1. [マイアカウント] で、[管理コントロールパネルを開く] を選択します。
2. [Storage (ストレージ)] で、[Change (変更)] を選択します。

3. [Storage Limit (ストレージの制限)] ダイアログボックスで、新規ユーザーに無制限または制限されたストレージのどちらかを付与するように選択します。
4. [Save Changes] (変更を保存) を選択します。

ストレージ設定の変更は、設定が変更された後に追加されたユーザーにのみ影響します。既存のユーザーに割り当てられたストレージの量は変更されません。既存のユーザーのストレージ制限を変更するには、「ユーザーの編集」をご参照ください。

IP 許可リスト

WorkDocs サイト管理者は、IP 許可リスト設定を追加して、サイトへのアクセスを許可された IP アドレスの範囲に制限できます。サイトごとに最大 500 個の IP 許可リスト設定を追加できます。

> **Note**
>
> 現在、[IP Allow List] (IP 許可リスト) は、IPv4 アドレスにしか使用できません。IP アドレス拒否リストは現在サポートされていません。

[IP Allow List] (IP 許可リスト) に IP 範囲を追加するには

1. [マイアカウント] で、[管理コントロールパネルを開く] を選択します。
2. [IP Allow List] (IP 許可リスト) で、[Change] (変更) を選択します。
3. [CIDR 値の入力] に、IP アドレス範囲のクラスレスドメイン間ルーティング (CIDR) ブロックを入力し、[追加] を選択します。
   - 1 つの IP アドレスからのアクセスを許可するには、CIDR プレフィックスとして /32 を指定します。
4. [Save Changes] (変更を保存) を選択します。
5. [IP Allow List] (IP 許可リスト) の IP アドレスからサイトに接続するユーザーは、アクセスが許可されます。許可されていない IP アドレスからサイトに接続しようとするユーザーには、unauthorized レスポンスが返されます。

> **Warning**
>
> 現在の IP アドレスを使用してサイトにアクセスすることをブロックする CIDR 値を入力した場合は、警告メッセージが表示されます。現在の CIDR 値で続行する場合は、現在の IP アドレスを使用したサイトへのアクセスがブロックされます。このアクションを取り消すには、AWS Support にお問い合わせください。

セキュリティ — シンプルなActiveDirectory サイト

このトピックでは、シンプルな ActiveDirectory サイトのさまざまなセキュリティ設定について説明します。ActiveDirectory Connector を使用するサイトを管理する場合は、次のセクションを参照してください。

セキュリティ設定を使用するには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [セキュリティ] まで下にスクロールし、 [変更] を選択します。

   [ポリシーの設定] ダイアログボックスが表示されます。次の表に、Simple ActiveDirectory サイトのセキュリティ設定を示します。

設定	説明
[共有可能リンクの設定を選択] で、次のいずれかを選択します。	
[サイトワイドまたはパブリック共有可能リンクを許可しない]	全ユーザーのリンク共有を無効にします。
[ユーザーにサイトワイド共有可能リンクの作成を許可するが、パブリック共有可能リンクの作成は許可しない]	リンク共有をサイトメンバーのみに制限します。マネージド ユーザーはこのタイプのリンクを作成できます。

設定	説明
[ユーザーにサイトワイド共有可能リンクの作成を許可するが、パブリック共有可能リンクを作成できるのはパワー ユーザーだけ]	マネージド ユーザーはサイトワイドリンクを作成できますが、パブリック リンクを作成できるのはパワー ユーザーだけです。パブリック リンクでは、インターネット上の誰にでもアクセスできます。
[すべてのマネージド ユーザーは、サイトワイドおよびパブリック共有可能リンクを作成できる]	マネージド ユーザーはパブリック リンクを作成できます。

[自動アクティベーション] で、チェックボックスをオンまたはオフにします。

[ディレクトリ内の全ユーザーが WorkDocs サイトに初回ログインするときに自動アクティベーションする。]	ユーザーがサイトに初回ログインしたときに、自動的にアクティベーションを行います。

[WorkDocs サイトへの新規ユーザーの招待を許可するユーザー]で、次のいずれかを選択します。

[新規ユーザーを招待できるのは管理者のみ]	[新規ユーザーを招待できるのは管理者のみ]
ユーザーは、ファイルやフォルダを共有することで、どこからでも新規ユーザーを招待できる	ファイルやフォルダをそのユーザーと共有することで、ユーザーが新規ユーザーを招待できるようにします。
[ユーザーは、ファイルまたはフォルダーを共有することで、いくつかの特定のドメインから新規ユーザーを招待できる。]	ユーザーは、ファイルまたはフォルダを共有することで、指定のドメインから新規人物を招待することができます。

[新規ユーザーのロールを設定] で、チェックボックスをオンまたはオフにします。

[ディレクトリからの新規ユーザーはマネージド ユーザーになる (デフォルトではゲスト ユーザー)]	ディレクトリの新規ユーザーをマネージド ユーザーに自動的に変換します。

4. 完了したら、[変更を保存] を選択します。

セキュリティ — ActiveDirectory Connector サイト

このトピックでは、ActiveDirectory Connector サイトのさまざまなセキュリティ設定について説明します。Simple ActiveDirectory を使用するサイトを管理している場合は、前のセクションを参照してください。

セキュリティ設定を使用するには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [セキュリティ] まで下にスクロールし、 [変更] を選択します。

   [ポリシーの設定] ダイアログボックスが表示されます。次の表に示すのは、ActiveDirectory Connector サイトのセキュリティ設定とその説明です。

設定	説明
[共有可能リンクの設定を選択] で、次のいずれかを選択します。	
[サイトワイドまたはパブリック共有可能リンクを許可しない]	選択すると、全ユーザーのリンク共有が無効になります。
[ユーザーにサイトワイド共有可能リンクの作成を許可するが、パブリック共有可能リンクの作成は許可しない]	リンク共有をサイトメンバーのみに制限します。マネージド ユーザーはこのタイプのリンクを作成できます。
[ユーザーにサイトワイド共有可能リンクの作成を許可するが、パブリック共有可能リンクを作成できるのはパワー ユーザーだけ]	マネージド ユーザーはサイトワイドリンクを作成できますが、パブリック リンクを作成できるのはパワー ユーザーだけです。パブリック リンクでは、インターネット上の誰にでもアクセスできます。
[すべてのマネージド ユーザーは、サイトワイドおよびパブリック共有可能リンクを作成できる]	マネージド ユーザーはパブリック リンクを作成できます。

設定	説明
[自動アクティベーション] で、チェックボックスをオンまたはオフにします。	
[ディレクトリ内の全ユーザーが WorkDocs サイトに初回ログインするときに自動アクティベーションする。]	ユーザーがサイトに初回ログインしたときに、自動的にアクティベーションを行います。
[WorkDocs サイトでディレクトリユーザーのアクティブ化を許可するユーザー] で、次のいずれかを選択します。	
[管理者のみがディレクトリから新規ユーザーをアクティベートする。]	管理者のみが新規ディレクトリユーザーをアクティブ化できます。
[ユーザーは、ファイルまたはフォルダーを共有して、ディレクトリから新規ユーザーを有効化できる]	ユーザーは、ファイルまたはフォルダをディレクトリユーザーと共有することで、ディレクトリユーザーをアクティブ化できます。
[ユーザーは、ファイルやフォルダを共有することで、複数の特定ドメインから新規ユーザーを招待できる]	ユーザーは特定ドメインのユーザーのファイルまたはフォルダーのみを共有できます。このオプションを選択した場合は、ドメインを入力する必要があります。
[WorkDocs サイトへの新規招待を許可するユーザー] で、次のいずれかを選択します。	
[外部ユーザーとの共有]	Enables administrators and users to invite new external users to your WorkDocs site.
[管理者のみが新規外部ユーザーを招待できる]	管理者のみが新規外部ユーザーを招待できます。
[すべてのマネージド ユーザーが新規外部ユーザーを招待できる]	マネージド ユーザーが外部ユーザーを招待できるようにします。

> **Note**
> 以下のオプションは、この設定を選択した後にのみ表示されます。

設定	説明
[パワー ユーザーのみが新規外部ユーザーを招待できる]	パワー ユーザーのみが新規外部ユーザーを招待できるようにします。

[新規ユーザーのロールを設定] で、1 つまたは両方のオプションを選択します。

[ディレクトリからの新規ユーザーはマネージド ユーザーになる (デフォルトではゲストユーザー)]	ディレクトリの新規ユーザーをマネージド ユーザーに自動的に変換します。
[新規外部ユーザーはマネージド ユーザーになる (デフォルトではゲストユーザー)]	新規外部ユーザーをマネージド ユーザーに自動的に変換します。

4. 完了したら、[変更を保存] を選択します。

復旧箱の保持期間

ユーザーがファイルを削除すると、WorkDocs はそのファイルをユーザーのごみ箱に 30 日間保存します。その後、WorkDocs はファイルを一時的なリカバリビンに 60 日間移動し、完全に削除します。一時復旧箱を見ることができるのは管理者のみです。サイトワイドデータ保持ポリシーを変更することで、サイト管理者は復旧箱の保持期間を最短 0 日、最長 365 日に変更できます。

復旧箱の保持期間を変更するには

1. [マイアカウント] で、[管理コントロールパネルを開く] を選択します。
2. [復旧箱の保持期間] の横にある [変更] を選択します。
3. ファイルを復旧箱に保持する日数を入力し、[保存] を選択します。

> **Note**
>
> デフォルトの保持期間は 60 日間です。0 ~ 365 日の期間を使用できます。

管理者は、WorkDocs がユーザーファイルを完全に削除する前に、リカバリビンからユーザーファイルを復元できます。

ユーザーのファイルを復元するには

1. [マイアカウント] で、[管理コントロールパネルを開く] を選択します。
2. [ユーザーを管理] で、ユーザーのフォルダアイコンを選択します。
3. [復旧箱] で、復元するファイルを選択し、[復旧] アイコンをクリックします。
4. [ファイルを復元] で、ファイルを復元する場所を選択し、[復旧] を選択します。

ユーザー設定の管理

ユーザーロールの変更、ユーザーの招待、有効化、無効化を含むユーザーの設定を管理できます。詳細については、「WorkDocs ユーザーの招待と管理」を参照してください。

WorkDocs Drive を複数のコンピュータにデプロイする

ドメインに参加しているマシンフリートがある場合は、グループポリシーオブジェクト (GPO) または System Center Configuration Manager (SCCM) を使用して WorkDocs Drive クライアントをインストールできます。 https://amazonworkdocs.com/en/clients からクライアントをダウンロードできます。

WorkDocs Drive では、すべての AWS IP アドレスに対してポート 443 で HTTPS アクセスが必要であることに注意してください。また、ターゲットシステムが WorkDocs Drive のインストール要件を満たしていることを確認します。詳細については、Amazon WorkDocs ユーザーガイドの「WorkDocs Drive のインストール」を参照してください。 Amazon WorkDocs

> **Note**
>
> GPO または SCCM を使用する際のベストプラクティスとして、ユーザーがログインした後に WorkDocs Drive クライアントをインストールします。

WorkDocs Drive の MSI インストーラは、以下のオプションのインストールパラメータをサポートしています。

- **`SITEID`** – 登録時にユーザーの WorkDocs サイト情報を事前に入力します。例えば、`SITEID=` *`####`*。
- **`DefaultDriveLetter`** – WorkDocs Drive のマウントに使用するドライブ文字を事前に入力します。例えば、`DefaultDriveLetter=` *`W`*。ユーザーごとに異なるドライブ名が必要であることを覚えておいてください。また、ユーザーは WorkDocs Drive を初めて起動した後、ドライブ名は変更できますが、ドライブ文字は変更できません。

次の例では、ユーザーインターフェイスと再起動なしで WorkDocs Drive をデプロイします。MSI ファイルのデフォルト名を使用していることにご注意ください。

```
msiexec /i "AWSWorkDocsDriveClient.msi" SITEID=your_workdocs_site_ID
DefaultDriveLetter=your_drive_letter  REBOOT=REALLYSUPPRESS /norestart /qn
```

WorkDocs ユーザーの招待と管理

デフォルトでは、サイトの作成中にディレクトリをアタッチすると、WorkDocs の自動アクティベーション機能により、そのディレクトリ内のすべてのユーザーがマネージドユーザーとして新しいサイトに追加されます。

WorkDocs では、マネージドユーザーは個別の認証情報を使用してログインする必要はなく、ファイルの共有や共同作業ができ、自動的に 1 TB のストレージが備わります。ただし、ディレクトリ内に一部のユーザーのみを追加したい場合は、自動アクティベーションをオフにできます。次のセクションのステップで、その方法を説明します。

さらにユーザーの招待、有効化、無効化、およびユーザーのロールと設定の変更を行うことが可能です。ユーザーをディレクトリ管理者に昇格することもできます。ユーザーの昇格についての情報は、「ユーザーを管理者に昇格させる」を参照してください。

これらのタスクは WorkDocs ウェブクライアントの管理者コントロールパネルで実行し、以下のセクションの手順でその方法について説明します。ただし、WorkDocs を初めて使用する場合は、数分待って、管理タスクに進む前にさまざまなユーザーロールについて学習してください。

内容

ユーザーロールの概要

WorkDocs では、次のユーザーロールを定義します。ユーザープロファイルを編集することにより、ユーザーのロールを変更できます。詳細については、「ユーザーの編集」を参照してください。

- 管理者: ユーザーの管理とサイト設定の定義のためのアクセス権限など、サイト全体の管理者権限のある有料ユーザー。ユーザーを管理者に昇格する方法については、「ユーザーを管理者に昇格させる」をご参照ください。
- [パワーユーザー]: 管理者からの権限の特別なセットを持つ有料ユーザー。パワーユーザーのアクセス許可を設定する方法についての詳細は、「セキュリティ — シンプルなActiveDirectory サイト」および「セキュリティ — ActiveDirectory Connector サイト」を参照してください。
- ユーザー: ファイルを保存し、WorkDocs サイトの他のユーザーとコラボレーションできる有料ユーザー。
- Guest user (ゲストユーザー): ファイルを表示できる無料ユーザー。ゲストユーザーをユーザー、パワーユーザー、または管理者というロールにアップグレードすることができます。

> **Note**
>
> ゲストユーザーの役割を変更する場合、元に戻せない1回限りのアクションが実行されます。

WorkDocs は、これらの追加のユーザータイプも定義します。

WS ユーザー

WorkSpaces WorkSpace が割り当てられているユーザー。

- すべての WorkDocs 機能へのアクセス
- 50 GB のデフォルトストレージ (有料で 1 TB にアップグレード可能)
- 月額料金なし

アップグレードされた WS ユーザー

WorkSpaces WorkSpace が割り当てられ、アップグレードされたストレージを持つユーザー。

- すべての WorkDocs 機能へのアクセス
- 1 TB のデフォルトストレージ (従量制の追加のストレージを利用できます)
- 月額料金の対象

WorkDocs ユーザー

WorkSpaces WorkSpace が割り当てられていないアクティブな WorkDocs ユーザー。 WorkSpaces WorkSpace

- すべての WorkDocs 機能へのアクセス
- 1 TB のデフォルトストレージ (従量制の追加のストレージを利用できます)
- 月額料金の対象

管理コントロールパネルを起動する

WorkDocs ウェブクライアントの管理コントロールパネルを使用して、自動アクティベーションのオンとオフを切り替え、ユーザーロールと設定を変更します。

管理者用コントロールパネルを開くには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。

> **Note**
>
> 一部のコントロールパネルのオプションは、クラウドディレクトリと接続ディレクトリで異なります。

自動アクティベーションをオフにする

ディレクトリ内のすべてのユーザーを新しいサイトに追加したくない場合や、新しいサイトに招待するユーザーに異なる権限とロールを設定したい場合は、自動アクティベーションをオフにします。自動アクティベーションをオフにすると、新しいユーザーをサイトに招待できるユーザー (現在のユーザー、パワー ユーザー、管理者) を決定することもできます。このステップでは、両方のタスクを実行する方法を説明します。

自動アクティベーション をオフにするには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [セキュリティ] まで下にスクロールし、 [変更] を選択します。

   [Policy Settings] (ポリシーの設定) ダイアログボックスが表示されます。
4. [Auto activation] (自動アクティベーション) で、 [Allow all users in your directory to be automatically activated upon their first login to your WorkDocs site] (WorkDocsサイトへの初回ログイン時に、ディレクトリ内のすべてのユーザーを自動的にアクティベーションすることを許可する) の横のチェックボックスをオフにします。

   [Who should be allowed to activate directory users in your WorkDocs site] (WorkDocs サイトでディレクトリユーザーをアクティベートすることを許可する人) でオプションは変更されます。現在のユーザーに新しいユーザーを招待させたり、パワーユーザーや他の管理者にその機能を与えることもできます。
5. オプションを選択し、 変更の保存 を選択します。

手順 1 ~ 4 を繰り返して、自動アクティベーションを再度有効にします。

リンク共有の管理

このトピックでは、リンク共有を管理する方法について説明します。WorkDocs ユーザーは、ファイルとフォルダへのリンクを共有することで、ファイルとフォルダを共有できます。ファイル リンクは組織の内外で共有できますが、フォルダリンクは組織内部でのみ共有できます。管理者は、リンクを共有できるユーザーを管理します。

リンク共有を有効にするには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。

3. [セキュリティ] まで下にスクロールし、 [変更] を選択します。

   [ポリシーの設定] ダイアログボックスが表示されます。
4. 「共有可能なリンクの設定を選択してください」で、次のオプションを選択します。

   - サイト全体または公開されている共有可能なリンクを許可しない-すべてのユーザーのリンク共有を無効にします。
   - サイト全体の共有可能なリンクの作成をユーザーに許可するが、公開共有可能なリンクの作成は許可しない — リンク共有をサイトメンバーのみに制限します。マネージドユーザーはこのタイプのリンクを作成できます。
   - ユーザーはサイト全体の共有可能なリンクを作成できますが、公開共有可能なリンクを作成できるのはパワーユーザーだけです。マネージドユーザーはサイト全体のリンクを作成できますが、パブリックリンクを作成できるのはパワーユーザーだけです。パブリックリンクでは、インターネット上の誰にでもアクセスできます。
   - すべてのマネージドユーザーは、サイト全体および公開共有可能なリンクを作成できます。マネージドユーザーは、公開リンクを作成できます。
5. [変更の保存] をクリックします。

自動アクティベーションを有効にしてユーザーの招待を制御する

自動アクティベーションを有効にすると (デフォルトではオンになっています) 、ユーザーが他のユーザーを招待できるようになります。以下のいずれかに権限を付与できます。

- すべてのユーザー
- パワーユーザー
- 管理者

権限を完全に無効にすることもできます。このステップでは、その方法を説明します。

招待の権限を設定するには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

   
2. [管理] で、[管理コントロールパネルを開く] を選択します。

3. [セキュリティ] まで下にスクロールし、 [変更] を選択します。

   [ポリシーの設定] ダイアログボックスが表示されます。

4. [WorkDocsサイトでディレクトリユーザーにアクティベートを許可できる人] で、[外部ユーザーとの共有] チェックボックスを選択し、チェックボックスの下にあるオプションのいずれかを選択し、[変更の保存] を選択します。

   —OR—

   誰にも新しいユーザーを招待させたくない場合は、チェックボックスをオフにして、[変更を保存] を選択します。

新しいユーザーの招待

ディレクトリに参加する新しいユーザーを招待できます。また、既存のユーザーが新しいユーザーを招待できるようにすることもできます。詳細については、このガイドの「セキュリティ — シンプルなActiveDirectory サイト」および「セキュリティ — ActiveDirectory Connector サイト」を参照してください。

新しいユーザーを招待するには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [ユーザーを管理] で、[ユーザーを招待] を選択します。
4. [ユーザーを招待] ダイアログボックスで、[誰を招待したいですか？] に招待者のメールアドレスを入力し、[送信] を選択します。招待者ごとに、このステップを繰り返します。

WorkDocs は各受信者に招待メールを送信します。このメールには、WorkDocs アカウントの作成方法に関するリンクと手順が含まれています。招待リンクは 30 日後に有効期限が切れます。

ユーザーの編集

ユーザー情報や設定を変更できます。

ユーザーを編集するには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [ユーザーを管理] で、ユーザー名の横にある鉛筆アイコン
   ( )
   を選択します。
4. [ユーザーを編集] ダイアログボックスで、次のオプションを編集することができます。

   [名] (クラウドディレクトリのみ)

   ユーザーの名前。

   [姓] (クラウドディレクトリのみ)

   ユーザーの姓。

   [ステータス]

   ユーザーが [アクティブ]か [非アクティブ]かどうかを指定します。詳細については、「ユーザーの無効化」をご参照ください。

   [Role] (ロール)

   人がユーザーであるか管理者であるかを指定します。また WorkSpace が割り当てられているユーザーをアップグレードまたはダウングレードすることもできます。詳細については、「ユーザーロールの概要」をご参照ください。

   [ストレージ]

   既存ユーザーのストレージ制限を指定します。
5. [変更を保存] を選択します。

ユーザーの無効化

ユーザーのステータスを [非アクティブ] に変更することで、ユーザーのアクセスを無効にします。

ユーザーのステータスを非アクティブに変更するには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [ユーザーを管理]で、ユーザー名の横にある鉛筆アイコン
(
)
を選択します。
4. [非アクティブ] を選択し、[変更を保存] を選択します。

非アクティブ化されたユーザーは WorkDocs サイトにアクセスできません。

> **Note**
>
> ユーザーを非アクティブステータスに変更しても、WorkDocs サイトからファイル、フォルダ、またはフィードバックは削除されません。ただし、アクティブユーザーに、非アクティブユーザーのファイルやフォルダを転送することができます。詳細については、「ドキュメントの所有権の委譲」を参照してください。

保留中のユーザーを削除する

Simple AD、 AWS マネージド Microsoft、AD Connector のユーザーは、保留中のステータスで削除できます。これらのユーザーの1人を削除するには、ユーザー名の横にあるごみ箱アイコン
(
)
を選択します。

WorkDocs サイトには、ゲストユーザーではないアクティブなユーザーが少なくとも 1 人必要です。すべてのユーザーを削除する必要がある場合は、サイト全体を削除してください。

登録されたユーザーを削除することはおすすめしません。代わりに、ユーザーが WorkDocs サイトにアクセスできないように、ユーザーのステータスをアクティブから非アクティブに切り替える必要があります。

ドキュメントの所有権の委譲

非アクティブユーザーのファイルやフォルダをアクティブユーザーに委譲できます。ユーザーを無効にする方法の詳細は、「ユーザーの無効化」を参照してください。

> ⚠ Warning
>
> このアクションは元に戻すことができません。

ドキュメントの所有権を委譲するには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [ユーザーを管理]で、非アクティブなユーザーを検索します。
4. 非アクティブなユーザーの名前の横にある鉛筆アイコン
   (✎)
   を選択します。
5. [ドキュメントの所有権の委譲] を選択して、新しい所有者の E メールアドレスを入力します。
6. [変更を保存] を選択します。

ユーザーリストのダウンロード

管理者コントロールパネルからユーザーのリストをダウンロードするには、WorkDocs Companion をインストールする必要があります。WorkDocs Companion をインストールするには、WorkDocs のアプリケーションと統合」を参照してください。

ユーザーのリストをダウンロードするには

1. WorkDocs クライアントの右上隅にあるプロファイルアイコンを選択します。

2. [管理] で、[管理コントロールパネルを開く] を選択します。
3. [ユーザーを管理] で、[ユーザーをダウンロード)] を選択します。
4. [ユーザーをダウンロード] で、次のいずれかのオプションを使って、ユーザーのリストを `.json` ファイルとしてデスクトップにエクスポートします。

   - すべてのユーザー
   - ゲストユーザー
   - WS ユーザー
   - ユーザー
   - パワーユーザー
   - 管理
5. WorkDocs は、以下のいずれかの場所にファイルを保存します。

   - Windows – `Downloads/WorkDocsDownloads`
   - macOS – *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

   > **Note**
   >
   > ダウンロードには時間がかかる場合があります。また、ダウンロードしたファイルは `/~users` フォルダには入りません。

これらのユーザーロールの詳細については、「ユーザーロールの概要」をご参照ください。

共有とコラボレーション

ユーザーは、リンクまたは招待を送信してコンテンツを共有することができます。外部共有を有効にすると、ユーザーは外部ユーザーと共同作業することもできます。

WorkDocs は、アクセス許可を使用してフォルダとファイルへのアクセスを制御します。システムは、ユーザーのロールに基づいて権限を適用します。

内容

リンクの共有

ユーザーはリンクを共有を選択すると、WorkDocs コンテンツのハイパーリンクをすばやくコピーして、組織内外の同僚や外部ユーザーと共有できます。ユーザーはリンクを共有するときに、以下のアクセスオプションのいずれかを許可するようにリンクを設定できます。

- WorkDocs サイトのすべてのメンバーは、 ファイルを検索、表示、コメントできます。
- リンクを持つユーザーは、WorkDocs サイトのメンバーではないユーザーでもファイルを表示できます。このリンクオプションでは、アクセス許可が表示のみに制限されます。

表示のアクセス権限のある受取人は、ファイルの表示のみが可能です。コメントのアクセス権限により、ユーザーは新しいファイルのアップロード、既存のファイルの削除などの更新オペレーションや削除オペレーションのコメントと実行が可能です。

デフォルトでは、すべての管理対象ユーザーがパブリックリンクを作成できます。この設定を変更するには、管理コントロールパネルから [Security] (セキュリティ) 設定を更新します。詳細については、「サイト管理者コントロールパネルからの WorkDocs の管理」を参照してください。

招待による共有

招待により共有を有効にすると、サイトユーザーは招待メールを送信することで、個々のユーザーやグループとファイルやフォルダーを共有できます。招待状には共有コンテンツへのリンクが含まれており、招待者は共有ファイルまたはフォルダを開くことができます。招待者は、それらのファイルやフォルダーを他のサイト メンバーや外部ユーザーと共有することもできます。

招待されたユーザーごとに権限レベルを設定できます。作成したディレクトリグループを使用して招待で共有するチームフォルダを作成することもできます。

> **Note**
>
> 共有招待状には、ネストされたグループのメンバーは含まれません。これらのメンバーを含めるには、そのメンバーを「招待により共有」リストに追加する必要があります。

詳細については、「サイト管理者コントロールパネルからの WorkDocs の管理」を参照してください。

外部共有

外部共有を使用すると、WorkDocs サイトのマネージドユーザーは、余分なコストをかけずにファイルやフォルダを共有し、外部ユーザーとコラボレーションできます。サイトユーザーは、受信者が WorkDocs サイトの有料ユーザーになることなく、外部ユーザーとファイルやフォルダを共有できます。外部共有を有効にすると、ユーザーは共有したい外部ユーザーの電子メール アドレスを入力し、適切なビューア共有権限を設定できます。外部ユーザーを追加すると、権限は閲覧者のみに制限され、他の権限は使用できなくなります。外部ユーザーは、共有ファイルやフォルダへのリンクを含むメール通知を受け取ります。リンクを選択すると、外部ユーザーはサイトに移動し、そこで認証情報を入力して WorkDocs にログインします。共有されるファイルやフォルダは [私と共有]ビューに表示されます。

ファイル所有者はいつでも共有アクセス権限を変更したり、外部ユーザーのアクセス権限をファイルやフォルダから削除したりすることができます。管理対象のユーザーが外部ユーザーとコンテンツを共有できるようにするには、サイト管理者がサイトの外部共有を有効にする必要があります。[Guest user] (ゲストユーザー) が共同編集者または共同所有者になるには、サイト管理者がそれらのユーザーを [User] (ユーザー) レベルにアップグレードする必要があります。詳細については、「ユーザーロールの概要」をご参照ください。

デフォルトでは、外部共有は有効になっており、すべてのユーザーが外部ユーザーを招待できます。この設定を変更するには、管理コントロールパネルから [Security] (セキュリティ) 設定を更新します。詳細については、「サイト管理者コントロールパネルからの WorkDocs の管理」を参照してください。

アクセス許可

WorkDocs は、アクセス許可を使用してフォルダとファイルへのアクセスを制御します。アクセス権はユーザーのロールに基づいて適用されます。

内容

ユーザーロール

ユーザーロールはフォルダとファイルの権限を制御します。以下のユーザーロールをフォルダレベルで適用できます。

- フォルダ所有者 – フォルダまたはファイルの所有者。
- フォルダ共同所有者 – 所有者によってフォルダまたはファイルの共同所有者として指定されたユーザーまたはグループ。
- フォルダ寄稿者 — フォルダへの無制限アクセス権限を持つ人。
- フォルダ表示者 — フォルダへのアクセスが制限されている (読み取り専用権限) を持つ人。

以下のユーザーロールを個々のファイルレベルで適用できます。

- 所有者 – ファイルの所有者。
- 共同所有者 – 所有者によってファイルの共同所有者として指定されたユーザーまたはグループ。
- Contributor* – ファイルに関するフィードバックの提供を許可されたユーザー。
- ビューワー – ファイルへのアクセスが制限されたユーザー (読み取り専用およびビューアクティビティのアクセス許可) 。

- 匿名表示者– 外部表示リンクを使用して共有されたファイルを表示できる、組織外部の登録されていないユーザー。特に明記されていない限り、匿名ビューワーにはビューワーと同じ読み取り専用アクセス許可があります。匿名ビューワーはファイルアクティビティを表示できません。

* コントリビューターは既存のファイルバージョンの名前を変更できません。ただし、別の名前のファイルの新しいバージョンをアップロードすることはできます。

共有フォルダのアクセス許可

共有フォルダのユーザーロールには、次のアクセス許可が適用されます。

> **Note**
>
> フォルダに適用されるアクセス許可は、そのフォルダ内のサブフォルダとファイルにも適用されます。

- 表示 – 共有フォルダの内容を表示します。
- サブフォルダを表示 – サブフォルダを表示します。
- 共有を表示 – フォルダを共有している他のユーザーを表示します。
- フォルダをダウンロード – フォルダをダウンロードします。
- サブフォルダを追加 – サブフォルダを追加します。
- 共有 – 最上位フォルダを他のユーザーと共有します。
- 共有を取り消す – 最上位フォルダの共有を取り消します。
- サブフォルダを削除 – サブフォルダを削除します。
- 最上位フォルダを削除 – 最上位共有フォルダを削除します。

	ビュー	サブフォルダを表示	共有を表示	フォルダをダウンロードします。	サブフォルダを追加	共有	共有を取り消す	サブフォルダを削除	最上位フォルダを削除
フォルダ所有者	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダ共有者	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダ寄稿者	✓	✓	✓	✓	✓				
フォルダ表示者	✓	✓	✓	✓					

共有フォルダ内のファイルのアクセス許可

共有フォルダ内のファイルのユーザーロールには、次のアクセス許可が適用されます。

- 注釈 –ファイルにフィードバックを追加します。
- 削除 – 共有フォルダのファイルを削除します。
- 名前を変更 — ファイルの名前を変更します。
- アップロード – ファイルの新しいバージョンをアップロードします。
- ダウンロード – ファイルをダウンロードします。これがデフォルトのアクセス許可です。ファイルのプロパティを使用して、共有ファイルのダウンロードを許可または拒否することができます。
- ダウンロードを抑止 – ファイルをダウンロードさせないようにします。

> **Note**
>
> - このオプションを選択しても、表示 権限を持つユーザーは引き続きファイルをダウンロードできます。これを防ぐには、共有フォルダを開いて、そのユーザーにダウンロードさせたくない各ファイルの [ダウンロードを許可] 設定をクリアします。
> - MP4 ファイルの所有者または共同所有者がそのファイルのダウンロードを抑止すると、寄稿者と表示者は Amazon WorkDocs ウェブクライアントでそのファイルを再生できなくなります。

- 共有 – 他のユーザーとファイルを共有します。
- 共有を取り消す – ファイルの共有を取り消します。
- 表示 – 共有フォルダのファイルを表示します。
- 共有を表示 –ファイルを共有している他のユーザーを表示します。
- 注釈を表示 – 他のユーザーからのフィードバックを表示します。
- アクティビティを表示 – ファイルのアクティビティ履歴を表示します。
- バージョンを表示 – ファイルの以前のバージョンを表示します。
- バージョンを削除 — ファイルの 1 つ以上のバージョンを削除します。
- バージョンを復元 — 削除したファイルの 1 つまたは複数のバージョンを復元します。
- すべてのプライベートコメントを表示 – 所有者/共同所有者は、コメントへの返信ではなくても、ドキュメントのすべてのプライベートコメントを見ることができます 。

	注釈	削除	名前を変更	アップロード	ダウンロード	ダウンロードを抑止	共有	共有を取り消す	ビュー	共有を表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除	バージョンを復元	すべてのプライベートコメントを表示**
ファイル所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダ所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	注釈	削除	名前を変更	アップロード	ダウンロード	ダウンロードを抑止	共有	共有を取り消す	ビュー	共有を表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除	バージョンを復元	すべてのプライベートコメントを表示**
の共同所有者**																
フォルダ寄稿者***	✓			✓	✓				✓	✓	✓	✓	✓			

	注釈	削除	名前を変更	アップロード	ダウンロード	ダウンロードを抑止	共有	共有を取り消す	ビュー	共有を表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除	バージョンを復元	すべてのプライベートコメントを表示 **
フォルダ表示者					✓				✓	✓		✓				
匿名表示者									✓	✓						

* この場合、ファイル所有者は、ファイルの元のバージョンを共有フォルダにアップロードしたユーザーです。このロールのアクセス許可は、共有フォルダ内のすべてのファイルではなく、所有ファイルにのみ適用されます。

** 所有者と共同所有者は、すべてのプライベートコメントを表示できます。寄稿者が見ることができるプライベートコメントは、それが自分のコメントへの応答である場合に限られます。

*** コントリビューターは既存のファイルバージョンの名前を変更できません。ただし、別の名前のファイルの新しいバージョンをアップロードすることはできます。

共有フォルダダにないファイルのアクセス許可

次の権限は、共有フォルダに存在しないファイルのユーザー ロールに適用されます。

- 注釈 –ファイルにフィードバックを追加します。
- 削除 –ファイルを削除します。
- 名前を変更 — ファイルの名前を変更します。
- アップロード – ファイルの新しいバージョンをアップロードします。
- ダウンロード – ファイルをダウンロードします。これがデフォルトのアクセス許可です。ファイルのプロパティを使用して、共有ファイルのダウンロードを許可または拒否することができます。
- ダウンロードを抑止 – ファイルをダウンロードさせないようにします。

> **Note**
>
> MP4 ファイルの所有者または共同所有者がそのファイルのダウンロードを抑止すると、寄稿者と表示者は Amazon WorkDocs ウェブクライアントでそのファイルを再生できなくなります。

- 共有 – 他のユーザーとファイルを共有します。
- 共有を取り消す – ファイルの共有を取り消します。
- 表示 –ファイルを表示します。
- 共有を表示 –ファイルを共有している他のユーザーを表示します。
- 注釈を表示 – 他のユーザーからのフィードバックを表示します。
- アクティビティを表示 – ファイルのアクティビティ履歴を表示します。
- バージョンを表示 – ファイルの以前のバージョンを表示します。
- バージョンを削除 — ファイルの 1 つ以上のバージョンを削除します。
- バージョンを復元 — 削除したファイルの 1 つまたは複数のバージョンを復元します。

	注釈	削除	名前を変更	アップロード	ダウンロード	ダウンロードを抑止	共有	共有を取り消す	ビュー	共有を表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除	バージョンを復元
所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
共同所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
寄稿者**	✓			✓	✓				✓	✓	✓	✓	✓		
表示者					✓				✓	✓		✓			
匿名表示者									✓	✓					

* ファイル所有者と共同所有者は、すべてのプライベートコメントを表示できます。寄稿者が見ることができるプライベートコメントは、それが自分のコメントへの応答である場合に限られます。

** 寄稿者は既存のファイルバージョンの名前を変更できません。ただし、別の名前のファイルの新しいバージョンをアップロードすることはできます。

共同編集の有効化

共同編集オプションは、[管理コントロールパネル] の [オンライン編集の設定] で有効にすることができます。

内容

Hancom ThinkFree の有効化

WorkDocs サイトの Hancom ThinkFree を有効にして、ユーザーが WorkDocs ウェブアプリケーションから Microsoft Office ファイルを作成して共同編集できるようにします。詳細については、「Editing with Hancom ThinkFree(Hancom ThinkFree で編集する)」をご参照ください。

Hancom ThinkFree は WorkDocs ユーザーに追加料金なしで利用できます。追加のライセンスやソフトウェアのインストールは必要はありません。

Hancom ThinkFree を有効にするには

[Admin control panel] (管理コントロールパネル) から、Hancom ThinkFree 編集を有効にします。

1. [My Account] (自分のアカウント) で、[Open admin control panel] (管理コントロールパネルを開く) を選択します。
2. [Hancom Online Editing] (Hancom オンライン編集) の [Change] (変更) を選択します。
3. [Enable Hancom Online Editing Feature] (Hancom オンライン編集機能の有効化) を選択し、利用規約を確認して、 [Save] (保存) を選択します。

Hancom ThinkFree を無効にするには

[Admin control panel] (管理コントロールパネル) から、Hancom ThinkFree 編集を無効にします。

1. [My Account] (自分のアカウント) で、[Open admin control panel] (管理コントロールパネルを開く) を選択します。

2. [Hancom Online Editing] (Hancom オンライン編集) の [Change] (変更) を選択します。
3. [Enable Hancom Online Editing Feature] (Hancom オンライン編集機能の有効化) チェックボックスをオフにし、[Save] (保存) を選択します。

[Office Online で開く] の有効化

WorkDocs サイトの Office Online で Open を有効にして、ユーザーが WorkDocs ウェブアプリケーションから Microsoft Office ファイルを共同編集できるようにします。

Open with Office Online は、Office Online で編集するライセンスを持つ Microsoft Office 365 Work または School アカウントも持っている WorkDocs ユーザーに追加料金なしで利用できます。詳細については、「Open with Office Online」(Office Online で開く) をご参照ください。

[Office Online で開く] を有効にするには

[Admin control panel] (管理コントロールパネル) から、[Office Online で開く] を有効にします。

1. [マイアカウント] で、[管理コントロールパネルを開く] を選択します。
2. [Office Online] で、[変更] を選択します。
3. [Office Onlineの有効化] を選択し、[保存] を選択します。

[Office Online で開く] を無効にするには

[管理コントロールパネル] から、[Office Online で開く] を無効にします。

1. [マイアカウント] で、[管理コントロールパネルを開く] を選択します。
2. [Office Online] で、[変更] を選択します。
3. [Office Onlineの有効化]チェックボックスをオフにし、[保存]を選択します。

WorkDocs へのファイルの移行

WorkDocs 管理者は、WorkDocs Migration Service を使用して、複数のファイルとフォルダを WorkDocs サイトに大規模に移行できます。WorkDocs Migration Service は、Amazon Simple Storage Service (Amazon S3) と連携します。これにより、部門別ファイル共有とホームドライブまたはユーザーファイル共有を WorkDocs に移行できます。

このプロセス中、WorkDocs は AWS Identity and Access Management (IAM) ポリシーを提供します。このポリシーを使用して、以下を実行するために WorkDocs Migration Service へのアクセスを許可する新しい IAM ロールを作成します。

- 指定した Amazon S3 バケットを読み取り、リストアップします。
- 指定した WorkDocs サイトを読み書きします。

ファイルとフォルダを WorkDocs に移行するには、次のタスクを実行します。作業を開始する前に、以下のアクセス権限が設定されていることを確認してください。

- WorkDocs サイトの管理者権限
- IAM ロールを作成するためのアクセス権限

WorkDocs サイトが WorkSpaces フリートと同じディレクトリに設定されている場合は、次の要件に従う必要があります。

- WorkDocs アカウントのユーザー名に Admin を使用しないでください。Admin は WorkDocs の予約済みユーザーロールです。
- WorkDocs 管理者ユーザータイプは、アップグレードされた WS ユーザーである必要があります。詳細については、「ユーザーロールの概要」および「ユーザーの編集」を参照してください。

> **Note**
>
> ディレクトリ構造、ファイル名、およびファイルコンテンツは、WorkDocs に移行するときに保持されます。ファイルの所有者とアクセス権限は維持されません。

タスク

ステップ 1: 移行するコンテンツの準備

コンテンツを移行用に用意するには

1. WorkDocs サイトのマイドキュメントで、ファイルとフォルダを移行するフォルダを作成します。
2. 次の点を確認します。
   - ソースフォルダに含まれるファイルとサブフォルダは 100,000 個以下。この制限を超えると、移行は失敗します。
   - 個々のファイルが 5 TB を超えない。
   - 各ファイル名は 255 文字以下にする必要があります。WorkDocs Drive は、フルディレクトリパスが 260 文字以下のファイルのみを表示します。

> **Warning**
>
> 名前に以下の文字が含まれるファイルやフォルダを移行しようとすると、エラーが発生し、移行プロセスが停止することがあります。このエラーが発生した場合は、[レポートをダウンロード] を選択して、エラー、移行に失敗したファイル、正常に移行されたファイルがリストされたログをダウンロードします。

- [末尾のスペース] - 例: ファイル名の末尾の余分なスペース。
- [先頭または末尾のピリオド] - 例: `.file`、`.file.ppt`、`.`、`..`、または `file.`
- [先頭または末尾のチルダ] - 例: `file.doc~`、`~file.doc`、または `~$file.doc`
- [**`.tmp`**で終わるファイル名] - 例: `file.tmp`
- [これらの大文字と小文字を区別する用語に完全に一致するファイル名] - `Microsoft User Data`、`Outlook files`、`Thumbs.db`、または `Thumbnails`

- [次の文字のいずれかを含んでいるファイル名] - * (アスタリスク)、/ (フォーワードスラッシュ)、\ (バックスラッシュ)、: (コロン)、< (小なり記号)、> (大なり記号)、? (疑問符)、| (縦線/パイプ)、" (二重引用符)、\202E (文字コード 202E)。

ステップ 2： Amazon S3 にファイルをアップロードする

Amazon S3 にファイルをアップロードするには

1. ファイルとフォルダをアップロードする AWS 新しい Amazon Simple Storage Service (Amazon S3) バケットをアカウントに作成します。Amazon S3 バケットは、WorkDocs サイトと同じ AWS アカウントと AWS リージョンに存在する必要があります。詳細については、「Amazon Simple Storage Service User Guide」(Amazon Simple Storage Service ユーザーガイド) の「Getting started with Amazon Simple Storage Service」(Amazon Simple ストレージサービスを開始する) を参照してください。
2. 前の手順で作成した Amazon S3 バケットにファイルをアップロードします。 AWS DataSync を使用してファイルやフォルダを Amazon S3 バケットにアップロードすることをお勧めします。DataSync は、追跡、報告、同期機能を追加で提供します。詳細については、 AWS DataSync ユーザーガイドの「 AWS DataSync の仕組み」および「DataSync のアイデンティティベースのポリシー (IAM ポリシー) の使用」を参照してください。

ステップ 3: 移行のスケジューリング

ステップ 1 と 2 を完了したら、WorkDocs Migration Service を使用して移行をスケジュールします。移行サービスでは、移行リクエストを処理し、移行を開始できる旨の E メールが送信されるまでに最大 1 週間かかる場合があります。E メールを受信する前に移行を開始すると、管理コンソールに待機することを指示するメッセージが表示されます。

移行をスケジュールすると、WorkDocs ユーザーアカウントのストレージ設定が自動的に Unlimited に変わります。

> **Note**
>
> WorkDocs ストレージ制限を超えるファイルを移行すると、追加コストが発生する可能性があります。詳細については、「WorkDocs の料金」を参照してください。

WorkDocs Migration Service は、移行に使用する AWS Identity and Access Management (IAM) ポリシーを提供します。このポリシーでは、指定した Amazon S3 バケットと WorkDocs サイトへのアクセス権を WorkDocs WorkDocsIAM ロールを作成します。また、Amazon SNS メール通知をサブスクライブして、移行リクエストがスケジューリングされたとき、およびそれが開始および終了されたときに更新を受信します。

移行をスケジューリングするには

1. WorkDocs コンソールから、アプリ、移行を選択します。
   - WorkDocs Migration Service に初めてアクセスする場合は、Amazon SNS E メール通知をサブスクライブするように求められます。サブスクライブし、受信したメールメッセージで確定してから、[Continue] (続行) を選択します。
2. 次に、[移行を作成] を選択します。
3. [ソースタイプ] で、[Amazon S3] を選択します。
4. [次へ] を選択します。
5. [Data Source & Validation] (データソースと検証) の [Sample Policy] (サンプルポリシー) で、提供されている IAM ポリシーをコピーします。
6. 前の手順でコピーした IAM ポリシーを使用して、以下のような新しい IAM ポリシーとロールを作成します。
   a. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
   b. [ポリシー]、[ポリシーの作成] を選択します。
   c. [JSON] を選択し、前にクリップボードにコピーしておいたポリシーを貼り付けます。
   d. [ポリシーの確認] を選択します。ポリシーの名前と説明を入力します。
   e. [Create policy] (ポリシーの作成) を選択します。
   f. [ロール]、[ロールの作成] を選択します。
   g. [別の AWS アカウント] を選択します。[アカウント ID] に、次のいずれかを入力します。
      - 米国西部 (バージニア北部) リージョンの場合は、899282061130 を入力します
      - 米国西部 (オレゴン) リージョンの場合は、814301586344 を入力します
      - アジアパシフィック (シンガポール) リージョンの場合は、900469912330 を入力します
      - アジアパシフィック (シドニー) リージョンの場合は、031131923584 を入力します
      - アジアパシフィック (東京) リージョンの場合は、178752524102 を入力します
      - 欧州 (アイルランド) リージョンの場合は、191921258524 を入力します

h. 作成した新しいポリシーを選択し、[次へ: 確認] を選択します。新しいポリシーが表示されない場合は、最新表示アイコンを選択します。

i. ロール名と説明を入力します。[ロールの作成] を選択します。

j. [ロール] ページの [ロール名]で、作成したロール名を選択します。

k. [概要]ページで、[CLI/API セッションの最大持続時間] を 12 時間に変更します。

l. [Role ARN] (ロール ARN) をクリップボードにコピーします。これは次のステップで使用します。

7. WorkDocs Migration Service に戻ります。[Data Source & Validation] (データソースと検証) の [Role ARN] (ロール ARN) で、前の手順でコピーした IAM ロールからのロール ARN を貼り付けます。
8. [Bucket] (バケット) では、ファイルの移行元の Amazon S3 バケットを選択します。
9. [次へ] を選択します。
10. 送信先 WorkDocs フォルダを選択する で、ファイルを移行する WorkDocs の送信先フォルダを選択します。
11. [次へ] を選択します。
12. [Review] (確認) の [Title] (タイトル) に、この移行の名前を入力します。
13. 移行の日付と時刻を選択します。
14. [Send] (送信) を選択します。

ステップ 4: 移行を追跡する

WorkDocs Migration Service ランディングページ内から移行を追跡できます。WorkDocs サイトからランディングページにアクセスするには、アプリ、移行を選択します。詳細を表示し進捗状況を追跡する移行を選択します。移行をキャンセルする必要がある場合は [移行をキャンセル] を選択できます。また、移行のタイムラインを更新するには [更新] を選択します。移行が完了した後は、[レポートをダウンロード] を選択して、正常に移行されたファイル、失敗したもの、エラーのログをダウンロードできます。

次のような移行の状態で移行のステータスを表します。

Scheduled (スケジュール済み)

移行がスケジューリングされていますがまだ開始されていません。予定された開始時刻の 5 分前までであれば、移行をキャンセルしたり、移行の開始時間を更新したりできます。

移行中

移行が進行中です。

Success (成功)

移行が完了しました。

一部成功

移行が一部成功しました。詳細については、移行の概要を表示し、提供されているレポートをダウンロードします。

失敗

移行に失敗しました。詳細については、移行の概要を表示し、提供されているレポートをダウンロードします。

キャンセル

移行がキャンセルされました。

ステップ 5: リソースをクリーンアップする

移行が完了したら、IAM コンソールから作成した移行ポリシーとロールを削除します。

IAM ポリシーとロールを削除するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. [ポリシー] を選択します。
3. 作成したロールを検索し、選択します。
4. [ポリシーアクション] で、[削除] を選択します。
5. [削除] を選択します。
6. [ロール] を選択します。
7. 作成したロールを検索し、選択します。
8. [ロールの削除]、[削除] を選択します。

スケジュールされた移行が開始されると、WorkDocs ユーザーアカウントのストレージ設定は自動的に Unlimited に変更されます。移行後、管理者コントロールパネルを使用してその設定を変更できます。詳細については、「ユーザーの編集」を参照してください。

WorkDocs の問題のトラブルシューティング

以下の情報は、WorkDocs に関する問題のトラブルシューティングに役立ちます。

問題

特定の AWS リージョンで WorkDocs サイトを設定できない

新しい WorkDocs サイトを設定する場合は、セットアップ中に AWS リージョンを選択します。詳細については、「WorkDocs の開始方法」で特定のユースケースのチュートリアルをご参照ください。

既存の Amazon VPC で WorkDocs サイトをセットアップしたい

新しい WorkDocs サイトを設定するときは、既存の Virtual Private Cloud (VPC) を使用してディレクトリを作成します。WorkDocs はこのディレクトリを使用してユーザーを認証します。

ユーザーがパスワードをリセットする必要がある

ユーザーはサインイン画面で [パスワードをお忘れですか?] を選択すれば、パスワードをリセットできます。

ユーザーが誤って機密文書を共有した

ドキュメントへのアクセスを取り消すには、ドキュメントの横にある [Share by invite] (招待により共有) を選択し、アクセスできなくなるユーザーを削除します。リンクを使用してドキュメントを共有した場合は、[リンクの共有] を選択してリンクを無効にします。

ユーザーが組織を退職し、ドキュメントの所有権を委譲しなかった

管理コントロールパネルで、ドキュメントの所有権を別のユーザーに委譲します。詳細については、「ドキュメントの所有権の委譲」を参照してください。

WorkDocs Drive または WorkDocs Companion を複数のユーザーにデプロイする必要がある

グループポリシーを使用して企業内の複数のユーザーにデプロイします。詳細については、「Amazon WorkDocs のアイデンティティおよびアクセス管理」を参照してください。WorkDocs Drive を複数のユーザーにデプロイする方法の詳細については、「」を参照してくださいWorkDocs Drive を複数のコンピュータにデプロイする。

オンライン編集が機能していない

WorkDocs Companion がインストールされていることを確認します。WorkDocs Companion をインストールするには、WorkDocs のアプリケーションと統合」を参照してください。

Amazon Business の WorkDocs の管理

WorkDocs for Amazon Business の管理者は、Amazon Business 認証情報を使用して https://workdocs.aws/ にサインインすることでユーザーを管理できます。

Amazon Business の WorkDocs に新しいユーザーを招待するには

1. https://workdocs.aws/ で Amazon Business 認証情報を使用してサインインします。
2. WorkDocs for Amazon Business ホームページで、左側のナビゲーションペインを開きます。
3. [Admin Settings] (管理者設定) を選択します。
4. [Add people] (ユーザーを追加) を選択します。
5. [Recipients] (受取人) に、招待するユーザーのメールアドレスまたはユーザー名を入力します。
6. (オプション) 招待メッセージをカスタマイズします。
7. [Done] (完了) を選択します。

WorkDocs for Amazon Business でユーザーを検索するには

1. https://workdocs.aws/ で Amazon Business 認証情報を使用してサインインします。
2. WorkDocs for Amazon Business ホームページで、左側のナビゲーションペインを開きます。
3. [Admin Settings] (管理者設定) を選択します。
4. [Search users] (ユーザー検索) で、ユーザーの名を入力し、**Enter** を押します。

WorkDocs for Amazon Business でユーザーロールを選択するには

1. https://workdocs.aws/ で Amazon Business 認証情報を使用してサインインします。
2. WorkDocs for Amazon Business ホームページで、左側のナビゲーションペインを開きます。
3. [Admin Settings] (管理者設定) を選択します。
4. [People] (人員) で、ユーザーの横にある [Role] (ロール) を選択して、ユーザーに割り当てます。

WorkDocs for Amazon Business でユーザーを削除するには

1. https://workdocs.aws/ で Amazon Business 認証情報を使用してサインインします。
2. WorkDocs for Amazon Business ホームページで、左側のナビゲーションペインを開きます。
3. [Admin Settings] (管理者設定) を選択します。

4. [People] (人員) の下で、省略記号 (...) を選択します。
5. [Delete] (削除) を選択します。
6. プロンプトが表示されたら、ユーザのファイルの転送先となる新しいユーザを入力し、[Delete] (削除) を選択します。

許可リストに追加する IP アドレスとドメイン

WorkDocs にアクセスするデバイスに IP フィルタリングを実装する場合は、次の IP アドレスとドメインを許可リストに追加します。これにより、WorkDocs と WorkDocs Drive が WorkDocs サービスに接続できるようになります。

- zocalo.ap-northeast-1.amazonaws.com
- zocalo.ap-southeast-2.amazonaws.com
- zocalo.eu-west-1.amazonaws.com
- zocalo.eu-central-1.amazonaws.com
- zocalo.us-east-1.amazonaws.com
- zocalo.us-gov-west-1.amazonaws.com
- zocalo.us-west-2.amazonaws.com
- awsapps.com
- amazonaws.com
- cloudfront.net
- *.aws.amazon.com
- amazonworkdocs.com
- console.aws.amazon.com
- cognito-identity.us-east-1.amazonaws.com
- firehose.us-east-1.amazonaws.com

IP アドレス範囲を使用する場合は、AWS 全般リファレンスの「AWS IP アドレス範囲」を参照してください。

ドキュメント履歴

以下の表は、2018 年 2 月以降の Amazon WorkDocs Administration Guide」 (Amazon WorkDocs 管理ガイド) の重要な変更点を説明しています。このドキュメントの更新に関する通知をするために、RSS フィードをサブスクライブすることができます。

変更	説明	日付
新しいファイル所有者の許可	管理者がバージョン削除権限とバージョン回復権限を付与できるようになりました。これらの権限は DeleteDocumentVersion API のリリースの一部です。	2022 年 7 月 29 日
WorkDocs バックアップ	コンポーネントがサポートされなくなったため、Amazon WorkDocs 管理ガイドから WorkDocs Backup ドキュメントを削除しました。 Amazon WorkDocs	2021 年 6 月 24 日
Amazon Business の WorkDocs の管理	WorkDocs for Amazon Business は、管理者によるユーザー管理をサポートしています。詳細については、「Amazon WorkDocs 管理ガイド」の「Amazon Business の Amazon WorkDocs の管理」を参照してください。	2020 年 3 月 26 日
「ファイルをAmazon WorkDocs に移行する」	WorkDocs 管理者は、WorkDocs Migration Service を使用して、複数のファイルとフォルダを WorkDocs サイトに大規模に移行できます。	2019 年 8 月 8 日

	詳細については、「Amazon WorkDocs 管理ガイド」の「WorkDocs へのファイルの移行」を参照してください。Amazon WorkDocs	
[IP allow list] (IP 許可リスト) の設定	IP 許可リスト設定は、IP アドレス範囲によって WorkDocs サイトへのアクセスをフィルタリングするために使用できます。詳細については、Amazon WorkDocs 管理ガイドの「IP allow list settings」(IP 許可リストの設定) を参照してください。	2018 年 10 月 22 日
Hancom ThinkFree	Hancom ThinkFree をお使いいただけます。ユーザーは、WorkDocs ウェブアプリケーションから Microsoft Office ファイルを作成して共同編集できます。詳細については、Amazon WorkDocs 管理ガイドの「Enabling Hancom ThinkFree」(Hancom ThinkFreeの有効化) を参照してください。	2018 年 6 月 21 日

[Office Online で開く]	[Office Online で開く] が使用可能になりました。ユーザーは、WorkDocs ウェブアプリケーションから Microsoft Office ファイルを共同編集できます。詳細については、Amazon WorkDocs 管理ガイドの「Enabling Open with Office Online」(Office Online で開くの有効化) を参照してください。	2018 年 6 月 6 日
トラブルシューティング	トラブルシューティングのトピックを追加しました。詳細については、「Amazon WorkDocs 管理ガイド」の「WorkDocs の問題のトラブルシューティング」を参照してください。 Amazon WorkDocs	2018 年 5 月 23 日
リカバリ用ごみ箱の保持期間の変更	リカバリ用ごみ箱の保持期間を変更できるようになりました。詳細については、Amazon WorkDocs 管理ガイドの「Recovery bin retention settings」(リカバリ用ごみ箱の保持設定) を参照してください。	2018 年 2 月 27 日