Amazon WorkDocs

管理ガイド

Amazon WorkDocs: 管理ガイド

Table of Contents

Amazon WorkDocs とは

Amazon WorkDocs は、完全マネージド型のセキュア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、強固な管理コントロールと、ユーザーの生産性を向上するための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。Amazon WorkDocs のクライアントアプリケーションは、ファイルのインターネットメディアタイプに応じて、さまざまな種類のファイルの表示に使用されます。Amazon WorkDocs では、一般的なドキュメント形式やイメージ形式がサポートされているほか、メディアタイプのサポートは定期的に追加されています。

詳細については、「Amazon WorkDocs」を参照してください。

Amazon WorkDocs へのアクセス

管理者は、Amazon WorkDocs コンソールを使用して Amazon WorkDocs サイトの作成および非アクティブ化を行います。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、「サイト設定の管理 (p. 32)」および「Amazon WorkDocs ユーザーの招待と管理 (p. 37)」を参照してください。

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。これらは、Amazon WorkDocs コンソールまたは管理ダッシュボードを使用することはありません。Amazon 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。
- macOS または Windows デスクトップ上のフォルダを Amazon WorkDocs ファイルと同期するために使用するドキュメント同期アプリケーション。
- ウェブページのイメージを Amazon WorkDocs ファイルに保存できるウェブクリッパーのブラウザ拡張機能。いくつかの人気の高いウェブブラウザ向けが用意されています。

ユーザーによる Amazon WorkDocs クライアントのダウンロード、ファイルの編集の方法、またサポートされるファイルタイプの詳細については、以下を参照してください。

- Amazon WorkDocs の開始方法
- ファイルの編集
- サポートされているファイルの種類

料金表

Amazon WorkDocs に前払い料金などの義務はありません。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、「料金表」を参照してください。

開始方法

Amazon WorkDocs を開始するには、次のチュートリアルのいずれかを試してください。

- クイックスタートの開始方法 (p. 20)
- Simple AD 標準設定の開始方法 (p. 22)
- 既存のディレクトリの開始方法 (p. 24)
- AD Connector の開始方法 (p. 26)
- AWS Managed Microsoft AD の開始方法 (p. 28)

Amazon WorkDocs に対して有効にされたディレクトリを持つ Amazon WorkSpaces 管理者アカウントを持っている場合、Amazon WorkDocs サイトにサインインして、[Admin control panel (管理コントロールパネル)] からセットアップを完了できます。詳細については、「ステップ 3: 管理コントロールパネルのセットアップを完了する (p. 24)」を参照してください。

Amazon WorkSpaces を使用して Amazon WorkDocs の使用を開始する方法の詳細については、Amazon WorkSpaces Administration Guideの「Amazon WorkSpaces 高速セットアップを開始する」を参照してください。Amazon WorkSpaces または Amazon EC2 インスタンスでの Amazon WorkDocs クライアントの使用の詳細については、Amazon VPC ユーザーガイドの「Amazon S3 のエンドポイント」を参照してください。

Amazon WorkDocs の前提条件

新しい Amazon WorkDocs サイトのセットアップ、既存のサイトの管理を行うには、以下のタスクを完了する必要があります。

タスク

- Sign up for AWS (p. 3)
- IAM ユーザーおよびグループを作成する (推奨) (p. 3)

Sign up for AWS

AWS アカウントからすべてのサービスにアクセスできますが、料金は使用したリソースに対してのみ発生します。

AWS アカウントをお持ちでない場合は、次に説明する手順に従ってアカウントを作成してください。

AWS にサインアップするには

1. https://aws.amazon.com/ を開き、[AWS アカウントの作成] を選択します。
2. オンラインの手順に従います。

AWS ルートアカウント認証情報により、AWS のサービスに対してお客様の身分が証明され、Amazon WorkDocs サイトなどの AWS リソースを無制限に使用できる許可が与えられます。

IAM ユーザーおよびグループを作成する (推奨)

セキュリティ認証情報を共有することなく、新しい Amazon WorkDocs サイトのセットアップや既存のサイトの管理を他のユーザーに対して許可するには、AWS Identity and Access Management (IAM) を使用します。アカウント所有者も含め、だれもが IAM ユーザーとして作業することをお勧めします。自分用に IAM ユーザーを作成し、その IAM ユーザーに管理者特権を与えて、それをすべての作業に使用します。

詳細については、「Amazon WorkDocs の Identity and Access Management (p. 4)」を参照してください。

Amazon WorkDocs のセキュリティ

AWS では、クラウドのセキュリティが最優先事項です。AWS のお客様は、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ーから利点を得られます。

セキュリティは、AWS とお客様の間の共有責任です。共有責任モデルでは、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 は、AWS クラウド内で 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責任を担います。また、AWS は、使用するサービスを安全に提供します。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の詳細については、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」を参照してください。
- クラウド内のセキュリティ – お客様の責任はお客様が使用する AWS のサービスによって決まります。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および規制などの他の要因についても責任を担います。

このドキュメントでは、Amazon WorkDocs を使用する際に責任共有モデルを適用する方法について説明します。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 Amazon WorkDocs を設定する方法について説明します。また、Amazon WorkDocs リソースのモニタリングやセキュリティ保護に役立つ他の AWS の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 Identity and Access Management

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コントロールするために役立つ AWS のサービスです。IAM 管理者は、Amazon WorkDocs リソースを使用するために認証 (サインイン) および承認 (アクセス許可を持つ) される者を制御します。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

Audience

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

サービスユーザー – ジョブを実行するために Amazon WorkDocs サービスを使用する場合は、管理者が必要なアクセス許可と認証情報を用意します。作業を実行するためにさらに多くの Amazon WorkDocs 機能を使用するとき、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解すると、管理者から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。Amazon WorkDocs の機能にアクセスできない場合は、「Amazon WorkDocs Identity and Access のトラブルシューティング (p. 13)」を参照してください。

サービス管理者 – 社内の Amazon WorkDocs リソースを担当している場合は、おそらく Amazon WorkDocs へのフルアクセスがあります。従業員がどの Amazon WorkDocs 機能とリソースアクセスする必要があるかを決定するのは管理者の仕事です。その後で、サービスユーザーのアクセス許可を変更するために、IAM 管理者にリクエストを送信する必要があります。IAM の基本概念については、このページの情報を確認します。お客様の会社で Amazon WorkDocs の IAM を利用する方法の詳細については、「Amazon WorkDocs と IAM の連携 (p. 9)」を参照して ください。

IAM 管理者 – IAM 管理者は、Amazon 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 Amazon 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、「Amazon WorkDocs アイデンティティベースのポリシーの例 (p. 11)」を参照して ください。

アイデンティティを使用した認証

認証は、アイデンティティ認証情報を使用して AWS にサインインする方法です。AWS マネジメントコンソール を使用したサインインの詳細については、IAM ユーザーガイド の「IAM ユーザーまたは ルートユーザー としての AWS マネジメントコンソール へのログイン」を参照してください。

AWS アカウントのルートユーザー、IAM ユーザーとして、または IAM ロールを引き受けて、認証されている (AWS にサインインしている) 必要があります。会社のシングルサインオン認証を使用することも、Google や Facebook を使用してサインインすることもできます。このような場合、管理者は以前に IAM ロールを使用して ID フェデレーションを設定しました。他の会社の認証情報を使用して AWS にアクセスした場合、ロールを間接的に割り当てられています。

AWS マネジメントコンソール に直接サインインするには、ルートユーザー E メールまたは IAM ユーザー名とパスワードを使用します。ルートユーザー または IAM ユーザーのアクセスキーを使用して AWS にプログラム的にアクセスできます。AWS では、SDK とコマンドラインツールを提供し、お客様の認証情報を使用して、リクエストに暗号で署名できます。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。これには、インバウンド API リクエストを認証するためのプロトコル、署名バージョン 4 を使用します。リクエストの認証の詳細については、AWS General Referenceの「署名バージョン 4 の署名プロセス」を参照してください。

使用する認証方法を問わず、追加のセキュリティ情報の提供を要求される場合もあります。たとえば、AWS では多要素認証 (MFA) を使用してアカウントのセキュリティを高めることを推奨しています。詳細については、IAM ユーザーガイドの「AWS での多要素認証 (MFA) の使用」を参照してください。

AWS アカウントのルートユーザー

AWS アカウントを初めて作成する場合は、このアカウントのすべての AWS サービスとリソースに対して完全なアクセス権限を持つシングルサインインアイデンティティで始めます。このアイデンティティは AWS アカウント ルートユーザー と呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでのサインインによりアクセスします。強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためだけに ルートユーザー を使用するというベストプラクティスに従います。その後、ルートユーザー認証情

報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

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特定のアクセス許可がある AWS アカウント内のアイデンティティです。IAM ユーザーは、ユーザー名とパスワード、アクセスキーのセットなど、長期的な認証情報を持つことができます。アクセスキーを生成する方法については、IAM ユーザーガイドの「IAM ユーザーのアクセスキーの管理」を参照してください。IAM ユーザーにアクセスキーを生成するとき、必ずキーペアを表示して安全に保存してください。後になって、シークレットアクセスキーを回復することはできません。新しいアクセスキーペアを生成する必要があります。

IAM グループは、IAM ユーザーのコレクション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、一度に複数のユーザーに対してアクセス許可を指定できます。多数の組のユーザーがある場合、グループを使用すると管理が容易になります。たとえば、IAM Admin 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アクセス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 人の特定の人または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、ロールでは一時的な認証情報が利用できます。詳細については、IAM ユーザーガイドの「IAM ユーザーの作成が適している場合 (ロールではなく)」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を持つ、AWS アカウント内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーに関連付けられていません。ロールを切り替えて、AWS マネジメントコンソール で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、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「IAM ロールの使用」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。

- 一時的な IAM ユーザーアクセス許可 – IAM ユーザーは、特定のタスクに対して複数の異なるアクセス許可を一時的に IAM ロールで引き受けることができます。
- フェデレーティッドユーザーアクセス – IAM ユーザーを作成する代わりに、AWS Directory Service、エンタープライズユーザーディレクトリ、またはウェブ ID プロバイダーに既存のアイデンティティを使用できます。このようなユーザーはフェデレーティッドユーザーと呼ばれます。AWS では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーティッドユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、IAM ユーザーガイド の「フェデレーティッドユーザーとロール」を参照してください。
- 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信頼済みプリンシパルに許可できます。ロールは、クロスアカウントアクセスを許可する主な方法です。ただし、一部の AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスでのロールとリソースベースのポリシーの違いの詳細については、IAM ユーザーガイドの「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- サービス間アクセス – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - プリンシパルアクセス許可 – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see in the Service Authorization Reference.

  - サービスロール – サービスロールは、サービスがお客様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。サービスロールは、お客様のアカウント内のみでアクセスを提供します。他のアカウントのサービスへのアクセス権を付与するためにサービスロールを使用することはできません。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの「AWS サービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- 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 リクエストを作成している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。AWS ロールを EC2 インスタンスに割り当て、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認証情報を取得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「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用してアクセス許可を付与する」を参照してください。

IAM ロールを使用するか IAM ユーザーを使用するかについては、IAM ユーザーガイド の「IAM ロールの作成が適している場合 (ユーザーではなく)」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

AWS でアクセスをコントロールするには、ポリシーを作成して IAM アイデンティティや AWS リソースにアタッチします。ポリシーは AWS のオブジェクトであり、ID やリソースに関連付けて、これらのアクセス許可を定義します。ルートユーザー または IAM ユーザーとしてサインインすることも、IAM ロールを引き受けることもできます。リクエストを行うと、AWS は関連する ID ベースまたはリソースベースのポリシーを評価します。ポリシーでのアクセス許可により、リクエストが許可されるか拒否されるかが決まります。大半のポリシーは JSON ドキュメントとして AWS 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 ポリシーの概要」を参照してください。

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

すべての IAM エンティティ (ユーザーまたはロール) は、アクセス許可のない状態からスタートします。言い換えると、デフォルト設定では、ユーザーは何もできず、自分のパスワードを変更することすらできません。何かを実行するアクセス許可をユーザーに付与するには、管理者がユーザーにアクセス許可ポリシーをアタッチする必要があります。また、管理者は、必要なアクセス許可があるグループにユーザーを追加できます。管理者がグループにアクセス許可を付与すると、そのグループ内のすべてのユーザーにこれらのアクセス許可が付与されます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションのアクセス許可を定義します。たとえば、`iam:GetRole` アクションを許可するポリシーがあるとします。このポリシーがあるユーザーは、AWS マネジメントコンソール、AWS CLI、または AWS API からロールの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

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the IAM ユーザーガイド.

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管理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、AWS アカウント内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロン

ポリシーです。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。管理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比較」を参照してください。

リソースベースのポリシー

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM role trust policies and Amazon S3 bucket policies. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

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 IAM の AWS 管理ポリシーを使用することはできません。

アクセスコントロールリスト

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ACL をサポートするサービスの例としては、Amazon S3、AWS WAF、Amazon VPC などがあります。ACL の詳細については、Amazon Simple Storage Service 開発者ガイドの「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 では、別のあまり一般的ではないポリシータイプもサポートしています。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アクセス許可を設定できます。

- 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のポリシーが IAM エンティティ (IAM ユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティの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アクセス許可は、エンティティの ID ベースのポリシーとそのアクセス許可の境界の共通部分です。`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は、アクセス許可の境界では制限されません。これらのポリシーのいずれかを明示的に拒否した場合、その許可は無効になります。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 (SCP) – SCP は、AWS Organizations で 組織や組織単位 (OU) に最大権限を指定する JSON ポリシーです。AWS Organizations は、お客様の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、一元的に管理するサービスです。組織内のすべての機能を有効にすると、サービス制御ポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP はメンバーアカウントのエンティティに対するアクセス許可を制限します (各 AWS アカウントのルートユーザー など)。Organizations および SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の動作」を参照してください。
- 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ティッドユーザーの一時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。結果として得られるセッションのアクセス許可は、ユーザーまたはロールの ID ベースのポリシーとセッションポリシーの共通部分です。また、リソースベースのポリシーからアクセス許可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、その許可は無効になります。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。

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アクセス許可を理解するのがさらに複雑になります。複数のポリシータイプが関連する場合にリクエストを許可するかどうか

を AWS で決定する方法の詳細については、IAM ユーザーガイドの「ポリシーの評価ロジック」を参照してください。

Amazon WorkDocs と IAM の連携

IAM を使用して、Amazon WorkDocs へのアクセスを管理するには、Amazon WorkDocs で使用できる IAM の機能を理解しておく必要があります。どのように Amazon WorkDocs その他 AWS サービスでは IAMと連携します。 AWS 機能するサービス IAM を IAM ユーザーガイド.

トピック

Amazon 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。Amazon WorkDocs では、特定のアクションがサポートされています。JSONポリシーで使用する要素の詳細については、以下を参照してください。 IAM JSON ポリシー要素の参照 を IAM ユーザーガイド.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

JSON ポリシーの `Action` 要素は、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を記述します。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。ただし、一致する API オペレーションを持たないアクセス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、従属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。

のポリシー アクション Amazon WorkDocs アクションの前に次のプレフィックスを使用します。`workdocs:`. たとえば、 Amazon WorkDocs `DescribeUsers` API 操作では、`workdocs:DescribeUsers` 行動に移します。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。Amazon WorkDocs は、このサービスで実行できるタスクを説明する独自の一連のアクションを定義します。

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 (*) を使用して複数のアクションを指定できます。たとえば、`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、以下のアクションを含めます。

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

次のリストを表示するには: Amazon WorkDocs アクション、参照 アクションの定義者 Amazon WorkDocs を IAM ユーザーガイド.

Resources

Amazon WorkDocs はリソースの指定をサポートしていません ARNs 方針に盛り込まれています。

条件キー

Amazon WorkDocs にはサービス固有条件キーがありませんが、いくつかのグローバル条件キーの使用がサポートされています。すべての AWS グローバル条件キー、参照グローバルジョウケンキー、ホソクジョウ AWS グローバル条件コンテキスト キー を IAM ユーザーガイド.

Examples

Amazon 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、「Amazon WorkDocs アイデンティティベースのポリシーの例 (p. 11)」を参照してください。

Amazon WorkDocs リソースベースのポリシー

Amazon 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。

Amazon WorkDocs タグに基づいた承認

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

Amazon WorkDocs の 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。

Amazon WorkDocs を使用した一時的な認証情報の使用

一時的な認証情報を使用して、フェデレーションでサインイン、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole または GetFederationToken などの AWS STS API オペレーションを呼び出します。

Amazon WorkDocs では、一時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ロール

サービスにリンクされたロールによって、AWS サービスが他のサービスのリソースにアクセスして自動的にアクションを完了できます。サービスにリンクされたロールは、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、サービスにリンクされた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 WorkDocs で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。

サービスロール

この機能では、サービスのロールをユーザーに代わって引き受けることをサービスに許可します。このロールにより、サービスは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、アクションを実行できます。サービスロールは、IAM アカウントに表示され、サービスによって所有されます。つまり、IAM 管理者は、このロールのアクセス許可を変更できます。ただし、これを行うことにより、サービスの機能が損なわれる場合があります。

Amazon WorkDocs は、サービスロールをサポートしていません。

Amazon WorkDocs アイデンティティベースのポリシーの例

デフォルトでは、IAM ユーザーおよびロールには、Amazon 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 や AWS CLI、AWS API を使用してタスクを実行することもできません。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アクセス許可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、管理者はそれらのアクセス許可が必要な IAM ユーザーまたはグループにそのポリシーをアタッチします。

_の作成方法を学ぶには IAM これらのJSONポリシー ドキュメントの例を使用したIDベースのポリシー。を参照してください。 [JSON] タブでのポリシーの作成 を IAM ユーザーガイド.

トピック

ポリシーのベストプラクティス

アイデンティティベースのポリシーは非常に強力です。アカウント内で、Amazon 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 アカウントに追加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のポリシーを作成または編集するときは、以下のガイドラインと推奨事項に従います。

- AWS 管理ポリシーの使用を開始する – Amazon WorkDocs の使用をすばやく開始するには、AWS 管理ポリシーを使用して、従業員に必要なアクセス許可を付与します。これらのポリシーはアカウントですでに有効になっており、AWS によって管理および更新されています。詳細については、『IAM ユーザーガイド』の「AWS 管理ポリシーを使用したアクセス許可の使用開始」を参照してください。
- 最小権限を付与する – カスタムポリシーを作成するときは、タスクの実行に必要なアクセス許可のみを付与します。最小限のアクセス権限から開始し、必要に応じて追加のアクセス権限を付与します。この方法は、寛容なアクセス権限で始め、後でそれらを強化しようとするよりも安全です。詳細については、「最小権限を付与する」 (IAM ユーザーガイド) を参照してください。
- 機密性の高いオペレーションのために MFA を有効にする – 追加のセキュリティとして、機密性の高いリソースや API オペレーションにアクセスする際に Multi-Factor Authentication (MFA) を使用することを IAM ユーザーに要求します。詳細については、『IAM ユーザーガイド』の「AWS のデバイスに多要素認証 (MFA) を使用」を参照してください。
- 追加のセキュリティとしてポリシー条件を使用する – 実行可能な範囲内で、アイデンティティベースのポリシーでリソースへのアクセスを許可する条件を定義します。たとえば、要求が発生しなければならない許容 IP アドレスの範囲を指定するための条件を記述できます。指定された日付または時間範囲内でのみリクエストを許可する条件を書くことも、SSL や MFA の使用を要求することもできます。ポリシー要素の詳細については、『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。

Amazon WorkDocs コンソールを使用して

Amazon WorkDocs コンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらの権限によって、 Amazon WorkDocs 資料を AWS アカウント。最低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 ユーザーまたは役割エンティティ。

これらのエンティティが Amazon WorkDocs 以下も接続してください。 AWS 管理されたポリシーをエンティティに送ります。ポリシーの添付の詳細については、以下を参照してください。 ユーザーへの権限の追加 を IAM ユーザーガイド.

- AmazonWorkDocsフルアクセス
- AWSディレクトリサービスフルアクセス
- AmazonEC2FullAccess

これらのポリシーは、IAMユーザーに Amazon WorkDocs AWS Directory Serviceの操作、Amazon EC2の操作など、 Amazon WorkDocs 適切に機能するために必要です。

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。

自分のアクセス許可の表示をユーザーに許可する

この例では、ユーザー ID にアタッチされたインラインおよび管理ポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了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": "*"
        }
    ]
}
```

Amazon 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

以下の AWS 管理の AmazonWorkDocsReadOnlyAccess ポリシーは、IAM ユーザーに Amazon 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、ユーザーに対して、Amazon

WorkDocs のすべての `Describe` オペレーションへのアクセス権を付与します。2つの Amazon EC2 オペレーションが必要なので、 Amazon WorkDocs は、 VPCs およびサブネットです。AWS Directory Service ディレクトリに関する情報を取得するには、AWS Directory Service の `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": "*"
        }
    ]
}
```

Amazon WorkDocs アイデンティティベースのその他のポリシーの例

IAM 管理者は、IAM ロールまたはユーザーに Amazon 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、以下を参照してください。 管理アプリケーションの認証とアクセス制御 を Amazon WorkDocs 開発者ガイド.

Amazon WorkDocs Identity and Access のトラブルシューティング

次の情報は、Amazon WorkDocs と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

Amazon WorkDocs でアクションを実行する権限がない

AWS マネジメントコンソール から、アクションを実行する権限がないと通知された場合、管理者に問い合わせ、サポートを依頼する必要があります。お客様のユーザー名とパスワードを発行したのが、担当の管理者です。

次のことを実行する権限がない: iam:PassRole

`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、管理者に問い合わせ、サポートを依頼する必要があります。お客様のユーザー名とパスワードを発行したのが、担当の管理者で

す。Amazon WorkDocs にロールを渡すことができるようにポリシーを更新するよう、管理者に依頼します。

一部の AWS 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せずに、既存のロールをサービスに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アクセス許可が必要です。

以下の例のエラーは、`marymajor` という IAM ユーザーがコンソールを使用して Amazon WorkDocs でアクションを実行しようする場合に発生します。ただし、アクションでは、サービスロールによって付与されたアクセス許可がサービスにある必要があります。メアリーには、ロールをサービスに渡すアクセス許可がありません。

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

この場合、メアリーは担当の管理者に `iam:PassRole` アクションを実行できるようにポリシーの更新を依頼します。

アクセスキーを表示する場合

IAM ユーザーアクセスキーを作成した後は、いつでもアクセスキー ID を表示できます。ただし、シークレットアクセスキーをもう一度表示することはできません。シークレットアクセスキーを紛失した場合は、新しいキーペアを作成する必要があります。

アクセスキーは、アクセスキー ID (例: `AKIAIOSFODNN7EXAMPLE`) とシークレットアクセスキー (例: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`) の 2 つの部分から構成されます。ユーザー名とパスワードと同様に、リクエストを認証するために、アクセスキー ID とシークレットアクセスキーの両方を使用する必要があります。ユーザー名とパスワードと同様に、アクセスキーをしっかり管理してください。

> Important
>
> 正規ユーザー ID を確認するためであっても、アクセスキーをサードパーティーに提供しないでください。提供すると、第三者がアカウントへの永続的アクセスを取得する場合があります。

アクセスキーペアを作成する場合、アクセスキー ID とシークレットアクセスキーを安全な場所に保存するように求めるプロンプトが表示されます。このシークレットアクセスキーは、作成時にのみ使用できます。シークレットアクセスキーを紛失した場合、新しいアクセスキーを IAM ユーザーに追加する必要があります。最大 2 つのアクセスキーを持つことができます。すでに 2 つある場合は、新しいキーペアを作成する前に、いずれかを削除する必要があります。手順を確認するには、IAM ユーザーガイドの「アクセスキーの管理」を参照してください。

管理者として Amazon WorkDocs へのアクセスを他のユーザーに許可したい

Amazon WorkDocs へのアクセスを他のユーザーに許可するには、アクセスを必要とする人またはアプリケーションの IAM エンティティ (ユーザーまたはロール) を作成する必要があります。ユーザーは、このエンティティの認証情報を使用して AWS にアクセスします。次に、Amazon WorkDocs の適切なアクセス許可を付与するポリシーを、そのエンティティにアタッチする必要があります。

すぐに開始するには、IAM ユーザーガイドの「IAM が委任した最初のユーザーおよびグループの作成」を参照してください 。

自分の AWS アカウント以外のユーザーに Amazon 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ユーザーが、リソースへのアクセスに使用できるロールを作成できます。ロールを引き受けるように信頼されたユーザーを指定することができます。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。

- Amazon WorkDocs でこれらの機能がサポートされるかどうかを確認するには、「Amazon WorkDocs と IAM の連携 (p. 9)」を参照してください。
- すべての所有してる AWS アカウントのリソースに対するアクセスを許可する方法については、IAM ユーザーガイドの「所有している別の AWS アカウントへのアクセス権を IAM ユーザーに提供」を参照してください。
- サードパーティーの AWS アカウントに対して自分のリソースへのアクセスを許可する方法については、IAM ユーザーガイドの「第三者が所有する AWS アカウントにアクセス権を付与する」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許可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でのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Amazon WorkDocs でのログ記録とモニタリング

Amazon WorkDocs のサイト管理者は、サイト全体のアクティビティフィードを表示、エクスポートできます。また、AWS CloudTrail を使用して Amazon 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 (p. 15)
- AWS CloudTrail を使用した Amazon WorkDocs API コールのログ記録 (p. 16)

サイト全体のアクティビティフィード

管理者は、サイト全体のアクティビティフィードを表示、エクスポートできます。この機能を使用するには、最初に Amazon WorkDocs Companion アプリをインストールする必要があります。Amazon WorkDocs Companion をインストールする方法については、「Amazon WorkDocs のアプリと統合」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、[アクティビティフィード] を選択します。
2. [フィルタ] を選択し、[サイト全体のアクティビティ] を表示するオプションを選択します。
3. [アクティビティタイプ] フィルタを選択し、必要に応じて [変更日] 設定を選択してから、[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できます。
5. [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。ファイルは次のいずれかの場所に保存されます。

   - 窓 – WorkDocsダウンロード フォルダーを ダウンロード フォルダー
   - macOS – `/users/username/WorkDocsDownloads/folder`

   適用したフィルタは、エクスポートされたファイルに反映されます。

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。詳細については、以下を参照してください。 アクティビティフィードの表示 を Amazon WorkDocs ユーザーガイド.

AWS CloudTrail を使用した Amazon WorkDocs API コールのログ記録

Amazon WorkDocs は、 AWS CloudTrailユーザー、役割、または AWS サービス Amazon WorkDocs. CloudTrail 次のすべてのAPI呼び出しをキャプチャ Amazon WorkDocs イベントとして、 Amazon WorkDocs コードコールから Amazon WorkDocs APIs. トレイルを作成する場合、 CloudTrail 件のイベントを Amazon S3 バケット、イベントを含む Amazon WorkDocs. 証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、Amazon WorkDocs に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、AWS CloudTrail User Guideを参照してください。

CloudTrail 内の Amazon WorkDocs 情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。Amazon 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 AWS の他のサービスのイベントと共に CloudTrail イベントとして [イベント履歴] に記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

Amazon 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、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべてのリージョンに適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した Amazon S3 バケットにログファイルが配信されます。さらに、より詳細な分析と CloudTrail ログで収集されたデータに基づいた行動のためにその他の 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 サポート対象のサービスと統合
- 設定 Amazon SNS 通知 CloudTrail
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「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 Amazon WorkDocs アクションは CloudTrail によってログに記録されます。これらのアクションは Amazon WorkDocs API リファレンス で説明されています。たとえば、`CreateFolder`、`DeactivateUser`、`UpdateDocument` セクションの呼び出しは、CloudTrail ログファイルにエントリを生成します。

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。この ID 情報は以下のことを確認するのに役立ちます。

- 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、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか.
- リクエストが、別の AWS サービスによって送信されたかどうか。

詳細については、 CloudTrail userIdentity 要素.

Amazon WorkDocs ログファイルエントリについて

証跡は、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できる設定です。CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは任意の送信元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ーなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API 呼び出し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。

Amazon WorkDocs が生成する CloudTrail エントリには、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 2 種類があります。この 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 ユーザーである点です。データプレーンエントリのユーザー ID は Amazon WorkDocs ディレクトリユーザーです。

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。

次の例は、Amazon 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のアクションを対象としていて、2 番目のレコードはデータプレーンのアクションを対象としています。

```
{
  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",
      "eventName" : "LogoutUser",
      "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検証

サードパーティーの監査では、複数の AWS コンプライアンスプログラムの一環として、Amazon WorkDocs のセキュリティとコンプライアンスの評価が行われます。これらのコンプライアンスプログラムには、SOC、PCI DSS、 FedRAMP、HIPAA、ISO 9001、ISO 27001、ISO 27017、および ISO 27018。

特定のコンプライアンスプログラムの範囲内の AWS サービスのリストについては、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

サードパーティーの監査レポートをダウンロードするには、AWS Artifact を使用します。詳細については、「AWS Artifact のレポートのダウンロード」を参照してください。

Amazon WorkDocs を使用する際のお客様のコンプライアンス責任は、データの機密性、企業のコンプライアンス目的、適用法規によって決まります。AWS は、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティおよびコンプライアンスのクイックスタートガイド – これらのデプロイメントガイドでは、アーキテクチャー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に重点を置いたベースライン環境を AWS にデプロイするための手順を説明します。
- HIPAA のセキュリティとコンプライアンスに関するホワイトペーパーを作成する – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスのリソース – このワークブックとガイドのコレクションは、お客様の業界や場所に適用される場合があります。
- AWS Config – この AWS サービスでは、自社プラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS Security Hub – この AWS サービスでは、AWS 内のセキュリティ状態を包括的に表示しており、セキュリティ業界の標準およびベストプラクティスへのコンプライアンスを確認するのに役立ちます。

Amazon WorkDocs での耐障害性

[AWS グローバルなインフラストラクチャは、 AWS 地域と空きゾーン。 AWSリージョンは、物理的に分離された複数の可用性ゾーンを提供します。このゾーンは、低レーテンシー、高スループット、および高度に冗長なネットワークで接続されます。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することなく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、および拡張性が優れています。

AWSのリージョンや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セキュリティ

マネージドサービスとして、 Amazon WorkDocs は、 AWS グローバルネットワークセキュリティ手順」を参照してください。 Amazon Web Services: セキュリティプロセスの概要 ホワイトペーパー。

AWS が公開している API コールを使用して、ネットワーク経由で Amazon WorkDocs にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、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の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 Service (AWS 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。

Amazon WorkDocs の開始方法

Amazon WorkDocs は、ディレクトリを使用して、ユーザーの組織情報とドキュメントを格納し管理します。クイックスタートまたは標準設定を使用して Simple AD ディレクトリを作成するか、オンプレミスディレクトリに接続する AD Connector ディレクトリを作成することができます。または、Amazon WorkDocs で既存の AWS ディレクトリの操作を有効にするか、Amazon WorkDocs で自動的にディレクトリを作成することができます。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、DoD などのコンプライアンスプログラムを適用するには、AWS Managed Microsoft AD ディレクトリをセットアップしてコンプライアンス要件に対応する必要があります。

内容

クイックスタートの開始方法

このチュートリアルでは、新しい Amazon WorkDocs サイトを設定し、クイックスタートで Simple AD ディレクトリを作成する方法を学習します。クイックスタートオプションは、以前に Amazon WorkDocs サイトを開設したことがない場合にのみ使用できます。

> Note
>
> 独自のディレクトリドメイン名を指定するか、ディレクトリで既存の仮想プライベートクラウド (VPC) を使用するなど、ディレクトリ構成をさらに制御する必要がある場合は、標準設定オプションを使用します。詳細については、「Simple AD 標準設定の開始方法 (p. 22)」を参照してください。

タスク

開始する前に

- Amazon WorkDocs サイトを作成または管理するには、AWS アカウントが必要です。ユーザーは、Amazon WorkDocs に接続して使用するためであれば AWS アカウントは必要としません。詳細については、「Amazon WorkDocs の前提条件 (p. 3)」を参照してください。

- 新しい Amazon WorkDocs サイトを起動するときは、管理者の姓名と電子メールアドレスを含むプロファイル情報を指定する必要があります。
- PCI、FedRAMP、DoD などのコンプライアンスプログラムを適用するには、Microsoft AD ディレクトリをセットアップしてコンプライアンス要件に対応する必要があります。代わりに、AWS Managed Microsoft AD の開始方法 (p. 28) の指示に従います。

ステップ 1: Amazon WorkDocs サイトを起動する

クイックスタートを使用すると、最初の Amazon WorkDocs サイトを数分で起動できます。

Amazon WorkDocs サイトを起動するには

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

   選択したリージョンで一度もディレクトリを作成または接続していない場合、Amazon WorkDocs 開始ページが表示されます。特定のリージョンでディレクトリを作成すると、開始ページが使用できなくなり、代わりに [WorkDocs サイトの管理] ページが表示されます。
2. Amazon WorkDocs 開始ページで [Get Started Now] を選択するか [Manage Your WorkDocs Sites] ページで [Create a New WorkDocs Site] を選択します。
3. [Get Started with WorkDocs] ページの [Quick Start] の横で、[Launch] を選択します。

ステップ 2: アクセスポイントを作成し、管理者を設定する

次の手順に従って、アクセスポイントを作成し、管理者を設定します。

アクセスポイントを作成して管理者を設定するには

1. [WorkDocs Quick Start] ページで [Access Point] に次の値を入力します。

   リージョン

   リージョンを確認します。

   [Site URL]

   Amazon WorkDocs サイトの URL を入力します。
2. [Set WorkDocs Administrator] に次の値を入力します。

   E メール

   ディレクトリ管理者の Eメールアドレス。ユーザー名としても使用されます。登録メールはこちらに送信されます。

   名

   ディレクトリ管理者の名。

   姓

   ディレクトリ管理者の姓。
3. [Complete Setup] を選択します。

   ディレクトリが接続され、Amazon WorkDocs サイトが作成されるまでに数分かかります。ディレクトリが正常に接続されると、サイトの [ステータス] 値が `Active` に変わります。

クイックスタートが、あなたの代わりに次のタスクを完了します。

- Virtual Private Cloud (VPC) を作成します。
- ユーザーおよび Amazon WorkDocs サイト情報を格納するために使用される VPC 内で Simple AD ディレクトリをセットアップします。
- ディレクトリの管理者アカウントを作成します。メールは、登録を完了する手順と共に管理者に送信されます。このアカウントを使用してディレクトリを管理します。
- 指定されたユーザーアカウントを作成し、ディレクトリに追加して、招待メールを送信します。

ステップ 3: 管理コントロールパネルのセットアップを完了する

管理者登録メールを受信したら、選択したクライアントを使用して Amazon WorkDocs サイトに接続し、管理コントロールパネルからセットアップを完了します。

管理コントロールパネルのセットアップを完了するには

1. 管理者登録メールで、リンクを使用して Amazon WorkDocs にサインインします。
2. [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。
3. 優先の言語、ストレージ、セキュリティ、リカバリ用ごみ箱の設定を変更します。詳細については、「サイト設定の管理 (p. 32)」を参照してください。
4. [Manage Users] で、[Invite Users] を選択します。ユーザー設定を編集することもできます。

詳細については、「Amazon WorkDocs ユーザーの招待と管理 (p. 37)」を参照してください。

Simple AD 標準設定の開始方法

このチュートリアルでは、標準設定を使用して Amazon WorkDocs サイトをセットアップし、クラウドに Simple AD ディレクトリを作成する方法を学習します。

タスク

開始する前に

- 『AWS Directory Service Administration Guide』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を適用するには、AWS Managed Microsoft AD ディレクトリをセットアップしてコンプライアンス要件に対応する必要があります。詳細については、「AWS Managed Microsoft AD の開始方法 (p. 28)」を参照してください。
- 新しい Amazon WorkDocs サイトを起動するときは、管理者の姓名と電子メールアドレスを含むプロファイル情報を指定する必要があります。

ステップ 1: Amazon WorkDocs サイトを起動する

次の手順に従い、標準設定を使用して Amazon WorkDocs サイトを起動します。

Amazon WorkDocs サイトを起動するには

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

   選択したリージョンで一度もディレクトリを作成または接続していない場合、Amazon WorkDocs 開始ページが表示されます。特定のリージョンでディレクトリを作成すると、開始ページが使用できなくなり、代わりに [WorkDocs サイトの管理] ページが表示されます。
2. Amazon WorkDocs 開始ページで [Get Started Now] を選択するか [Manage Your WorkDocs Sites] ページで [Create a New WorkDocs Site] を選択します。
3. [Get Started with WorkDocs] ページの [Standard Setup] の横で、[Launch] を選択します。

ステップ 2: ディレクトリを作成し、管理者を設定する

次の手順に従って、Simple AD ディレクトリを作成し、管理者を設定します。

Simple AD ディレクトリを作成するには

1. [Set up a Directory] ページで、[Create Simple AD] を選択します。
2. [Access Point] で次の値を入力し、[Continue] を選択します。

   リージョン

   リージョンを確認します。

   [Site URL]

   Amazon WorkDocs サイトの URL を入力します。
3. [Directory Details] で次の値を入力します。

   Directory DNS

   ディレクトリの完全修飾名。例: `corp.example.com`。

   NetBIOS name

   ディレクトリの NetBIOS 名。例: `CORP`。
4. [Set WorkDocs Administrator] に次の値を入力します。

   E メール

   ディレクトリ管理者の Eメールアドレス。ユーザー名としても使用されます。登録メールはこちらに送信されます。

   名

   ディレクトリ管理者の名。

   姓

   ディレクトリ管理者の姓。
5. [VPC Details] に [Set up a new VPC on my behalf] を選択して、Amazon WorkDocs が VPC を作成して設定するようにします。代わりに既存の VPC を使用するには、[Select an existing VPC to use with WorkDocs] を選択し、次の値を入力します。

VPC

ディレクトリが作成される VPC。

Subnets

ディレクトリが作成される VPC のサブネット。2 つのサブネットは、異なるアベイラビリティゾーンに存在している必要があります。[No Preference] を選択すると、2 つの異なるサブネットがランダムに選択されます。

6. ディレクトリ情報を確認し、必要な変更を加えます。情報が正しい場合は、[Create Directory] を選択します。

   ディレクトリが接続され、Amazon WorkDocs サイトが作成されるまでに数分かかります。ディレクトリが正常に接続されると、サイトの [ステータス] 値が `Active` に変わります。

ステップ 3: 管理コントロールパネルのセットアップを完了する

管理者登録メールを受信したら、選択したクライアントを使用して Amazon WorkDocs サイトに接続し、管理コントロールパネルからセットアップを完了します。

管理コントロールパネルのセットアップを完了するには

1. 管理者登録メールで、リンクを使用して Amazon WorkDocs にサインインします。
2. [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。
3. 優先の言語、ストレージ、セキュリティ、リカバリ用ごみ箱の設定を変更します。詳細については、「サイト設定の管理 (p. 32)」を参照してください。
4. [Manage Users] で、[Invite Users] を選択します。ユーザー設定を編集することもできます。

詳細については、「Amazon WorkDocs ユーザーの招待と管理 (p. 37)」を参照してください。

既存のディレクトリの開始方法

このチュートリアルでは、既存の AWS Directory Service ディレクトリを有効にして Amazon WorkDocs サイトを設定する方法を学習します。

タスク

開始する前に

- 現在のリージョン内に既存の AWS Directory Service ディレクトリが必要です。これは、Simple AD ディレクトリまたは AD Connector ディレクトリのいずれかです。
- PCI、FedRAMP、DoD などのコンプライアンスプログラムを適用するには、AWS Managed Microsoft AD ディレクトリをセットアップしてコンプライアンス要件に対応する必要があります。詳細については、「AWS Managed Microsoft AD の開始方法 (p. 28)」を参照してください。

- 新しい Amazon WorkDocs サイトを起動するときは、管理者のプロファイル情報を指定する必要があります。この情報には、名、姓、E メールアドレスが含まれます。Amazon 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、Amazon WorkDocs の予約されたユーザーロールです。

ステップ 1: Amazon WorkDocs サイトを起動する

次の手順に従い、既存の AWS Directory Service ディレクトリを使用して Amazon WorkDocs サイトを起動します。

Amazon WorkDocs サイトを起動するには

1. Amazon WorkDocs コンソール (https://console.aws.amazon.com/zocalo/) を開きます。
2. [Manage Your WorkDocs Sites] ページで、[Create a New WorkDocs Site] を選択します。

ステップ 2: ディレクトリを有効にし、管理者を設定する

次の手順に従って、既存のディレクトリを有効にし、管理者を設定します。

既存のディレクトリを有効にするには

1. [Select a Directory] ページで、[Available Directories] リストから AWS Directory Service ディレクトリを選択して、[Enable Directory] を選択します。
2. [Set WorkDocs Administrator] ページで、AWS Directory Service ディレクトリから Amazon WorkDocs 管理者となるユーザー名を入力し、[Select Administrator] を選択します。

   ディレクトリが接続され、Amazon WorkDocs サイトが作成されるまでに数分かかります。ディレクトリが正常に接続されると、サイトの [ステータス] 値が `Active` に変わります。

デフォルトでは、ディレクトリ内のすべてのユーザーがアクティブ Amazon WorkDocs ユーザーとしてアカウントに追加されます。ユーザーは、Amazon WorkDocs を使用していつでもサインインし、使用を開始できます。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 (p. 37)」を参照してください。

ステップ 3: 管理コントロールパネルのセットアップを完了する

管理者登録メールを受信したら、選択したクライアントを使用して Amazon WorkDocs サイトに接続します。その後、管理コントロールパネルからセットアップを完了します。

管理コントロールパネルのセットアップを完了するには

1. 管理者登録メールで、リンクを使用して Amazon WorkDocs にサインインします。
2. [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。
3. 優先の言語、ストレージ、セキュリティ、リカバリ用ごみ箱の設定を変更します。詳細については、「サイト設定の管理 (p. 32)」を参照してください。
4. (オプション) [Manage Users] で、[Invite Users] を選択します。ユーザー設定を編集することもできます。

詳細については、「Amazon WorkDocs ユーザーの招待と管理 (p. 37)」を参照してください。

AD Connector の開始方法

このチュートリアルでは、AWS Directory ServiceAD Connector ディレクトリを使用してオンプレミスディレクトリに接続する Amazon WorkDocs サイトを設定する方法を学習します。

タスク

開始する前に

- 『AWS Directory Service Administration Guide』の「AD Connector 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。
- 新しい Amazon WorkDocs サイトを起動するときは、管理者のプロファイル情報を指定する必要があります。この情報には、名、姓、E メールアドレスが含まれます。Amazon 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、Amazon WorkDocs の予約されたユーザーロールです。

ステップ 1: Amazon WorkDocs サイトを起動する

次の手順に従って Amazon WorkDocs サイトを起動し、オンプレミスディレクトリに接続します。

Amazon WorkDocs サイトを起動するには

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

   選択したリージョンで一度もディレクトリを作成または接続していない場合、Amazon WorkDocs 開始ページが表示されます。特定のリージョンでディレクトリを作成すると、開始ページが使用できなくなり、代わりに [WorkDocs サイトの管理] ページが表示されます。
2. Amazon WorkDocs 開始ページで [Get Started Now] を選択するか [Manage Your WorkDocs Sites] ページで [Create a New WorkDocs Site] を選択します。
3. [Get Started with WorkDocs] ページの [Standard Setup] の横で、[Launch] を選択します。

ステップ 2: ディレクトリを接続する

AWS Directory ServiceAD Connector ディレクトリを使用してオンプレミスディレクトリに接続するには、次の手順を実行します。

ディレクトリに接続するには

1. [Set up a Directory] ページの AD Connectorで、[CreateAD Connector] を選択します。
2. [Directory Details] で次の値を入力し、[Continue] を選択します。

Directory DNS

オンプレミスのディレクトリの完全修飾名。例 :corp.example.com。Amazon WorkDocs はこのディレクトリ内のユーザーアカウントにのみアクセスできます。ユーザーアカウントを親ディレクトリ (例: example.com) に含めることはできません。

NetBIOS Name

オンプレミスディレクトリの NetBIOS の名前。例: CORP。

Account Username

オンプレミスディレクトリのユーザーのユーザー名。

Account Password

オンプレミスのユーザーアカウント用のパスワード。

[Confirm Password]

オンプレミスのユーザーアカウント用のパスワードを再度入力します。これは、ディレクトリに接続する前に、入力エラーを防止するために必要です。

DNS アドレス

オンプレミスのディレクトリの DNS サーバーまたはドメインコントローラの IP アドレス。このサーバーは、以下で指定する各サブネットからアクセスできる必要があります。

3. [Access Point] で、次の値を入力します。

   リージョン

   リージョンを確認します。

   [Site URL]

   Amazon WorkDocs サイトの URL を入力します。

4. [VPC Configuration] で、次の値を入力します。

   VPC

   ディレクトリが接続されている VPC。

   Subnets

   オンプレミスディレクトリに接続するために使用する VPC のサブネット。2 つのサブネットは、異なるアベイラビリティゾーンに存在している必要があります。

5. ディレクトリ情報が正しいことを確認し、[Connect Directory] を選択します。

   ディレクトリが接続され、Amazon WorkDocs サイトが作成されるまでに数分かかります。ディレクトリが正常に接続されると、サイトの [ステータス] 値が `Active` に変わります。

デフォルトでは、ディレクトリ内のすべてのユーザーがアクティブ Amazon WorkDocs ユーザーとしてアカウントに追加されます。ユーザーは、Amazon WorkDocs を使用していつでもサインインし、使用を開始できます。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 (p. 37)」を参照してください。

ステップ 3: 管理コントロールパネルのセットアップを完了する

管理者登録メールを受信したら、選択したクライアントを使用して Amazon WorkDocs サイトに接続し、管理コントロールパネルからセットアップを完了します。

管理コントロールパネルのセットアップを完了するには

1. 管理者登録メールで、リンクを使用して Amazon WorkDocs にサインインします。
2. [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。
3. 優先の言語、ストレージ、セキュリティ、リカバリ用ごみ箱の設定を変更します。詳細については、「サイト設定の管理 (p. 32)」を参照してください。
4. (オプション) [Manage Users] で、[Invite Users] を選択します。ユーザー設定を編集することもできます。

詳細については、「Amazon WorkDocs ユーザーの招待と管理 (p. 37)」を参照してください。

AWS Managed Microsoft AD の開始方法

このチュートリアルでは、オンプレミス AWS Managed Microsoft AD ディレクトリに接続して Amazon WorkDocs サイトを設定する方法を学習します。

> Note
>
> PCI、FedRAMP、DoD などのコンプライアンスプログラムを適用するには、AWS Managed Microsoft AD ディレクトリをセットアップしてコンプライアンス要件に対応する必要があります。

タスク

開始する前に

- AWS Managed Microsoft AD を作成する必要があります。詳細については、「Microsoft AD ディレクトリの作成方法」を参照してください。
- AWS Directory Service と AWS Managed Microsoft AD との間に信頼関係を作成する必要があります。詳細については、「信頼関係を作成する場合」を参照してください。
- 新しい Amazon WorkDocs サイトを起動するときは、管理者のプロファイル情報を指定する必要があります。この情報には、名、姓、E メールアドレスが含まれます。Amazon 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、Amazon WorkDocs の予約されたユーザーロールです。

ステップ 1: Amazon WorkDocs サイトを起動する

次の手順に従い Amazon WorkDocs サイトを起動します。

Amazon WorkDocs サイトを起動するには

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

   選択したリージョンで一度もディレクトリを作成または接続していない場合、Amazon WorkDocs 開始ページが表示されます。特定のリージョンでディレクトリを作成すると、開始ページが使用できなくなり、代わりに [WorkDocs サイトの管理] ページが表示されます。

2. Amazon WorkDocs 開始ページで [Get Started Now] を選択するか [Manage Your WorkDocs Sites] ページで [Create a New WorkDocs Site] を選択します。
3. [Get Started with WorkDocs] ページの [Standard Setup] の横で、[Launch] を選択します。

ステップ 2: AWS Managed Microsoft AD を有効にし、管理者を設定する

次の手順に従って、AWS Managed Microsoft AD を有効にし、管理者を設定します。

AWS Managed Microsoft ADを有効にするには

1. 利用可能なディレクトリのリストから、Amazon WorkDocs サイトとして使用する AWS Managed Microsoft AD を選択します。

   Note

   このサイトが AWS Managed Microsoft AD と同じリージョンに作成されていることを確認してください。
2. [Enable directory] を選択します。
3. [Set WorkDocs Administrator] ページで、AWS Managed Microsoft AD ディレクトリから Amazon WorkDocs 管理者となるユーザー名を入力し、[Select Administrator] を選択します。

   ディレクトリが接続され、Amazon WorkDocs サイトが作成されるまでに数分かかります。ディレクトリが正常に接続されると、サイトの [ステータス] 値が `Active` に変わります。

デフォルトでは、ディレクトリ内のすべてのユーザーがアクティブ Amazon WorkDocs ユーザーとしてアカウントに追加されます。ユーザーは、Amazon WorkDocs を使用していつでもサインインし、使用を開始できます。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 (p. 37)」を参照してください。

ステップ 3: 管理コントロールパネルのセットアップを完了する

管理者登録メールを受信したら、選択したクライアントを使用して Amazon WorkDocs サイトに接続し、管理コントロールパネルからセットアップを完了します。

管理コントロールパネルのセットアップを完了するには

1. 管理者登録メールで、リンクを使用して Amazon WorkDocs にサインインします。
2. [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。
3. 優先の言語、ストレージ、セキュリティ、リカバリ用ごみ箱の設定を変更します。詳細については、「サイト設定の管理 (p. 32)」を参照してください。
4. (オプション) [Manage Users] で、[Invite Users] を選択します。ユーザー設定を編集することもできます。

詳細については、「Amazon WorkDocs ユーザーの招待と管理 (p. 37)」を参照してください。

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 が登録されているものと同じディレクトリに結合されているコンピュータから 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。Amazon WorkDocs 管理者は、AWS 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することができます。詳細については、『AWS Directory Service Administration Guide』の「シングルサインオン」を参照してください。

Amazon WorkDocs 管理者がシングルサインオンを有効にしたら、Amazon WorkDocs サイトのユーザーも、シングルサインオンを許可するようウェブブラウザの設定を変更する必要があります。詳細については、『AWS Directory Service Administration Guide』の「IE および Google Chrome でのシングルサインオン」および「Firefox で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

以下の手順を実行して、AD Connector ディレクトリの多要素認証を有効にすることができます。

> Note
>
> 多要素認証は、Simple AD ディレクトリでは使用できません。

多要素認証を有効にするには

1. Amazon WorkDocs コンソール (https://console.aws.amazon.com/zocalo/) を開きます。
2. [Manage Your WorkDocs Sites] ページで、目的のサイトを選択し、[Actions]、[Manage MFA] の順に選択します。
3. 以下の値を入力して、[Update MFA] を選択します。

   Multi-Factor Authentication の有効化

   オンにすると、多要素認証が有効になります。

   [RADIUS サーバーの IP アドレス]

   RADIUS サーバーエンドポイントの IP アドレス、または、RADIUS サーバーロードバランサーの IP アドレス。複数の IP アドレスをカンマで区切って入力できます (192.0.0.0,192.0.0.12 など)。

   ポート

   RADIUS サーバーが通信のために使用しているポート。オンプレミスネットワークでは、AD Connector サーバーからのデフォルトの RADIUS サーバーポート (1812) を介した受信トラフィックが許可されている必要があります。

   [Shared secret code]

   RADIUS エンドポイントの作成時に指定された共有シークレットコード。

   [共有シークレットコードの確認]

   RADIUS エンドポイントの共有シークレットコードを確認します。

   プロトコル

   RADIUS エンドポイントの作成時に指定されたプロトコルを選択します。

   [サーバータイムアウト]

   RADIUS サーバーのレスポンスを待つ時間 (秒) 。これは 1 ~ 60 の範囲の値にする必要があります。

最大再試行回数

RADIUS サーバーとの通信を試みる回数。これは 0 ~ 10 の範囲の値にする必要があります。

多要素認証は、[RADIUS Status] が [Enabled] に変わると使用できます。Multi-Factor Authentication のセットアップ中は、ユーザーが Amazon WorkDocs サイトにログインすることはできません。

ユーザーを管理者に昇格する

Amazon WorkDocs コンソールを使用して、ユーザーを管理者に昇格します。昇格するには、ユーザーがアクティブである必要があります。ユーザーのアクティブ化の詳細については、「ユーザーの編集 (p. 38)」を参照してください。

ユーザーを管理者に昇格するには

1. Amazon WorkDocs コンソール (https://console.aws.amazon.com/zocalo/) を開きます。
2. [Manage Your WorkDocs Sites] ページで、目的のディレクトリを選択し、[Actions]、[Set an Administrator] の順に選択します。
3. [Set WorkDocs Administrator] ページで、昇格するユーザー名を入力して、[Set Administrator] を選択します。

Amazon WorkDocs 管理ダッシュボードを使用して、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 (p. 38)」を参照してください。

サイト設定の管理

管理者は、サイトのコンテンツや E メール通知で使用する言語の選択、ストレージ制限の設定、リカバリ用ごみ箱の保持ポリシーの指定などの、サイト全体の設定を管理できます。管理者は、パブリック共有、招待、新規ユーザーのサイトセキュリティ設定を変更することもできます。

優先言語設定

サイトのコンテンツ、および E メール通知に使用する言語を指定します。

言語の設定を変更するには

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. [Preferred Language Settings (使用する言語の設定)] で、使用する言語を選択します。

Hancom Online Editing と Office Online

Admin コントロールパネルから Hancom Online Editing および Office Online の設定を有効または無効にできます。詳細については、「共同編集の有効化 (p. 45)」を参照してください。

ストレージ

新しい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. [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. [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、新しい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] 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 (p. 38)」を参照してください。

IP 許可リスト

Amazon WorkDocs サイト管理者は、許可された IP アドレスの範囲へのサイトアクセスを制限するために、IP 許可リストの設定を追加できます。サイトあたり最大 32 個の IP 許可リストの設定を追加できます。

> Note
>
> 現在、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 許可リストに IP 範囲を追加するには

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. [IP 許可リスト] で、[変更] を選択します。
3. [CIDR 値の入力] で、許可リストへの IP アドレス範囲の Classless Inter-Domain Routing (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] を選択します。
5. 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 サポートにお問い合わせください。

セキュリティ – パブリック共有の設定

管理コントロールパネルの [Security (セキュリティ)] で、[Who should be allowed to create publicly shareable links? (パブリックに共有可能なリンクの作成をだれに許可しますか?)] を選択して、組織外のユーザーへのファイル表示リンクの送信を許可するユーザーを指定します。次の設定から選択します。

パブリック共有なし

ユーザーは組織外の誰にも表示リンクを送信できません。

[All managed users can share publicly (すべての管理されたユーザーがパブリックに共有できます)]

すべてのユーザーは組織外の誰にでも表示リンクを送信できます。

パワーユーザーのみがパブリックに共有できます

パワーユーザーのみが組織外の人物に表示リンクを送信できます。

セキュリティ – 招待の設定

[Who should be allowed to join your WorkDocs site? (WorkDocs サイトへの参加が許可されるユーザー)] の以下の設定から選択します。

[Users can invite new people from anywhere by sharing files or folders with them]

ユーザーは、ファイルまたはフォルダを共有することで、組織外の新しい人物を任意の場所から招待することができます。

[Users can invite new people from a few specific domains by sharing files or folders with them]

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しい人物を招待することができます。

セキュリティ – 外部招待

[Who should be allowed to invite external users to your WorkDocs site? (WorkDocs サイトへの外部ユーザーの招待が許可される相手)] の以下の設定から選択します。

Only administrators can invite new external users

管理者のみが Amazon WorkDocs を使用するように外部ユーザーを招待できます。

All managed users can invite new external users

すべてのユーザーが Amazon WorkDocs を使用するように新しい外部ユーザーを招待できます。

[Only Power users can invite new external users (パワーユーザーのみが新しい外部ユーザーを招待できます)]

パワーユーザーのみが Amazon WorkDocs を使用するように新しい外部ユーザーを招待できます。

ごみ箱の保持期間

ユーザーによって削除されたファイルは、ユーザーのごみ箱に 30 日間保存されます。その後、ファイルは一時的にごみ箱に移動され、60 日間保存されてから完全に削除されます。ごみ箱は管理者のみに表示されます。サイトの管理者は、サイト全体のデータ保持ポリシーを変更することにより、最大 365 日までごみ箱の保持期間を変更できます。ファイルは、保持期間の終了時に完全に削除されます。

ごみ箱の保持期間を変更するには

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. [Recovery bin retention (リカバリ用ごみ箱の保持期間)] の横から、[Change (変更)] を選択します。
3. ファイルをリカバリ用ごみ箱に保持する日数を入力し、[Save (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。これは 0 ~ 365 日に変更できます。

ユーザーファイルが完全に削除される前に、リカバリ用ごみ箱から復元できます。

ユーザーのファイルを復元するには

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. [Manage Users (ユーザーの管理)] で、ユーザーのフォルダアイコンを選択します。
3. [Recovery bin (リカバリ用ごみ箱)] で、復元するファイルを選択し、[復元] アイコンをクリックします。
4. [ファイルの復元] で、ファイルを復元する場所を選択し、[復元] 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、「Amazon WorkDocs ユーザーの招待と管理 (p. 37)」を参照してください。

サイトの削除

Amazon WorkDocs コンソールを使用して、Amazon WorkDocs サイトを削除します。

> Warning
>
> サイトを削除するとすべてのユーザー情報と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. Amazon WorkDocs コンソール (https://console.aws.amazon.com/zocalo/) を開きます。
2. 必要に応じて、ナビゲーションバーから必要な AWS リージョンを選択します。詳細については、『アマゾン ウェブ サービス全般のリファレンス』の「リージョンとエンドポイント」を参照してください。
3. [WorkDocs サイトの管理] で、削除するサイトを選択します。[アクション] を選択してから、[WorkDocs サイトの削除] を選択します。
4. [Delete Selected WorkDocs Site (選択した WorkDocs サイトの削除)] ダイアログボックスで、同時にユーザーディレクトリも削除するかどうかを選択します。

   - [ユーザーディレクトリも削除する] を選択し、オンプレミス Microsoft Active Directory の AWS Directory Service Simple AD または AD Connector を削除します。ディレクトリを削除するには、そのディレクトリが他の AWS アプリケーションで有効になっていないことが必要です。詳細については、『AWS Directory Service Administration Guide』の「Simple AD ディレクトリの削除」または「AD Connector ディレクトリの削除」を参照してください。
5. 適切なサイトを削除しようとしていることを確認し、確認フィールドに「DELETE」と入力して、[WorkDocs サイトの削除] 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。

   > Note
   >
   > Amazon WorkDocs の独自のディレクトリを指定しなかった場合、ディレクトリは自動的に作成されています。Amazon WorkDocs サイトを削除する際は、ディレクトリを削除するか、他の AWS アプリケーション用に使用しない限り、自動的に作成されたディレクトリに対して課金されます。料金の詳細については、他のディレクトリタイプの料金表に関する記事を参照してください。

複数のコンピュータへの Amazon WorkDocs Drive のデプロイ

ドメイン結合された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 Amazon WorkDocs Drive クライアントをインストールできます。クライアントは、https://amazonworkdocs.com/en/clients からダウンロードできます。

使用するにつれて、Amazon WorkDocs Drive ではすべての AWS IP アドレスに対してポート 443 で HTTPS アクセスが必要です。また、ターゲットシステムが Amazon WorkDocs Drive のインストール要件を満たしていることも確認する必要があります。詳細については、Amazon WorkDocs Drive の「 のインストール」を参照してください。Amazon WorkDocs ユーザーガイド

> **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 Amazon WorkDocs Drive クライアントをインストールします。

の MSI インストーラは次のオプションインストールパラメータをサポートします。Amazon WorkDocs Drive

- **`SITEID`** – ユーザーの登録時に Amazon WorkDocs サイトの情報を事前に入力します。例: `SITEID=site-name`.
- **`DefaultDriveLetter`** – Amazon 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: `DefaultDriveLetter=W`。 各ユーザーには、異なるドライブ文字が必要です。また、ユーザーは Amazon WorkDocs Drive を初めて起動した後、ドライブ名を変更できますが、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なしで、再起動なしで Amazon 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することに注意してください。

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

Amazon WorkDocs ユーザーの招待と管理

ユーザーロールの変更、ユーザーの招待、有効化、無効化、ユーザー設定の変更は、Amazon WorkDocs Web クライアントの管理コントロールパネルの [Manage Users (ユーザーの管理)] で行うことができます。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。詳細については、「ユーザーを管理者に昇格する (p. 31)」を参照してください。

管理コントロールパネルを開くには、Amazon WorkDocs の [My Account] で、[Open admin control panel] を選択します。

> Note
>
> 管理者コントロールパネルのオプションの一部は、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。

目次

ユーザーロールの概要

Amazon WorkDocs では次のユーザーロールが定義されます。[User profile] を編集することで、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 (p. 38)」を参照してください。

- Admin: 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する (p. 31)」を参照してください。
- Power user: 管理者が特別なアクセス権限を付与できる、サイトの有料ユーザー。Power user のアクセス許可を設定する方法の詳細については、「セキュリティ – パブリック共有の設定 (p. 33)」および「セキュリティ – 外部招待 (p. 34)」を参照してください。
- User: Amazon WorkDocs サイトのファイルを保存して他のユーザーと共同作業できる有料ユーザー。
- Guest user: ファイルを表示できる無料ユーザー。Guest user は、User、Power user、または Administrator にアップグレードできます。

  > Note
  >
  > [Guest user] ロールを他の 3 つのロールのいずれかに変更することは、1 回限りの操作であり、元に戻すことはできません。

Amazon WorkDocs では、以下のユーザータイプも定義します。

WS ユーザー

Amazon WorkSpaces WorkSpace が割り当てられたユーザー。

- すべての Amazon WorkDocs 機能にアクセス
- 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

Amazon WorkSpaces WorkSpace が割り当てられ、アップグレードされたユーザー。

- すべての Amazon WorkDocs 機能にアクセス
- 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

Amazon WorkDocs ユーザー

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

- すべての Amazon WorkDocs 機能にアクセス
- 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

新しいユーザーの招待

管理コントロールパネルからディレクトリに参加するように新しいユーザーを招待します。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、「セキュリティ – 招待の設定 (p. 33)」を参照してください。

新しいユーザーを招待するには

1. 管理者の認証情報を使用して Amazon WorkDocs にサインインします。
2. [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。
3. [Manage Users] で、[Invite Users] を選択します。
4. [Invite Users (ユーザーの招待)] ユーザーの招待ダイアログボックスで、[Who would you like to invite? (招待するユーザー)] に招待者の E メールアドレスを入力し、[Send (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。

リンクと Amazon WorkDocs アカウントの作成方法を記載した招待メールがそれぞれの受取人に送信されます。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

ユーザーを編集することによって、既存のユーザー情報と設定を変更できます。

ユーザーを編集するには

1. 管理者の認証情報を使用して Amazon WorkDocs にサインインします。
2. [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。
3. [Manage Users (ユーザーの管理)] で、ユーザー名の横にある鉛筆アイコン () を選択します。
4. [Edit User] ダイアログボックスで、次の次のオプションを編集できます。

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を指定します。詳細については、「ユーザーの無効化 (p. 39)」を参照してください。

ロール

ユーザーがユーザーか管理者かを指定します。Amazon WorkSpaces WorkSpace が割り当てられた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 (p. 37)」を参照してください。

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. [Save Changes] 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できます。

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. 管理者の認証情報を使用して Amazon WorkDocs にサインインします。
2. [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。
3. [Manage Users (ユーザーの管理)] で、ユーザー名の横にある鉛筆アイコン (✎) を選択します。
4. [Inactive] を選択し、[Save Changes] を選択します。

非アクティブのユーザーは、Amazon WorkDocs サイトにアクセスできなくなります。

Note

ユーザーを非アクティブステータスに変更しても、ユーザーのファイルやフォルダ、Amazon WorkDocs サイトからのフィードバックは削除されません。ただし、ファイルやフォルダをアクティブユーザーに委譲することはできます。詳細については、「ドキュメントの所有権の委譲 (p. 40)」を参照してください。

保留中のユーザーを削除する (Simple AD のみ)

[Pending (保留中)] ステータスの Simple AD ユーザーのみ削除することができます。これらのうち、いずれかのユーザーを削除するには、ユーザー名の横にあるごみ箱アイコン (🗑) を選択します。

Amazon WorkDocs サイトには、ゲストユーザーではないアクティブユーザーが少なくとも 1 人存在する必要があります。すべてのユーザーを削除する場合は、Amazon WorkDocs サイト全体を削除する必要があります。

登録されたユーザーを削除することはお勧めできません。代わりに、ユーザーが Amazon 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。ユーザーを非アクティブにする方法について詳しくは、「ユーザーの無効化 (p. 39)」を参照してください。

ドキュメントの所有権を委譲するには

1. 管理者の認証情報を使用して Amazon WorkDocs にサインインします。
2. [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。
3. [Manage Users (ユーザーの管理)] 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. [Transfer Document Ownership] を選択し、ファイルを転送するアクティブユーザーの Eメールアドレスを入力します。
6. [Save Changes] を選択します。

   Warning

   このアクションは元に戻すことができません。

ユーザーリストのダウンロード

[Admin control panel (管理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、Amazon WorkDocs Companion アプリをインストールする必要があります。Amazon WorkDocs Companion をインストールする方法については、「Amazon WorkDocs のアプリと統合」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. 管理者の認証情報を使用して Amazon WorkDocs にサインインします。
2. [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。
3. [Manage Users (ユーザーの管理)] で、[Download user (ユーザーのダウンロード)] を選択します。
4. [Download user (ユーザーのダウンロード)] 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
   - 管理者
5. ファイルは次のいずれかの場所に保存されます。

   - Windows – PC のダウンロードフォルダの WorkDocsDownloads フォルダ
   - macOS – `/users/username/WorkDocsDownloads/folder`

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 (p. 37)」を参照してください。

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できます。外部共有が有効になると、外部ユーザーと共同作業を行うことができます。

Amazon WorkDocs はアクセス許可の使用を通じて、フォルダおよびファイルへのアクセスを制御します。アクセス許可はユーザーのロールに基づいて適用されます。

目次

共有中

ユーザーが Amazon WorkDocs でコンテンツを共有する方法はいくつかあります。

リンクの共有

ユーザーは、[Share a Link (リンクの共有)] を選択して Amazon WorkDocs コンテンツへのハイパーリンクをすばやくコピーし、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。

- Amazon WorkDocs サイトのすべてのメンバーはファイルの検索、表示、コメント付けができます。
- リンクがわかっていれば、Amazon WorkDocs サイトのメンバーでない場合でも、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、「サイト設定の管理 (p. 32)」を参照してください。

招待により共有

ユーザーは、[Share by invite (招待により共有)] を選択し、E メールアドレスを使用して他のユーザーを招待することで、ファイルやフォルダを共有できます。ユーザーは、招待されたユーザーに対してそれぞれ適切なアクセス許可を設定することもできます。招待されたユーザーは、コンテンツが共有されたことを通知する招待 E メールを自動的に受け取ります。E メールのリンクをクリックすると、共有ファイルが開きます。ユーザーは他のサイトメンバーや外部ユーザーとファイルやフォルダを共有できます。

ユーザーは、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。

外部共有

外部共有により、Amazon WorkDocs サイトの管理対象のユーザーは、ファイルやフォルダを共有したり、余分なコストをかけずに外部ユーザーと簡単に共同作業したりできます。サイトのユーザーは、受取

人を Amazon WorkDocs サイトの有料ユーザーにすることなく、外部ユーザーとファイルやフォルダを共有できます。外部共有が有効な場合、ユーザーは共有先となる外部ユーザーの E メールアドレスを入力し、ビューワーの共有アクセス権限を適切に設定できます。外部ユーザーを追加すると、アクセス権限はビューワーのみに制限され、他の権限は使用できません。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 E 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誘導され、そこで Amazon WorkDocs にログインするための認証情報を入力します。共有されるファイルやフォルダは [Shared with me] ビューに表示されます。

いつでも、ファイル所有者は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 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] 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 (p. 37)」を参照してください。

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、「サイト設定の管理 (p. 32)」を参照してください。

アクセス許可

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

目次

ロール

フォルダおよびファイルの両方のアクセス許可は、ユーザーロールに基づいて付与されます。Amazon WorkDocs で定義され、フォルダに適用されるロールを以下に示します。

- フォルダ所有者 – フォルダまたはファイルの所有者。
- フォルダ共有者 – 所有者によってフォルダまたはファイルの共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 – フォルダが共有され、フォルダへのアクセスは制限されていないユーザー。
- フォルダ表示者 – フォルダが共有されたが、フォルダへのアクセスが制限されている (表示のみ) ユーザー。

次のロールがファイルに適用されます。

- 所有者 – ファイルの所有者。
- 共有者 – 所有者によってファイルの共有者として指定されたユーザーまたはグループ。
- 寄稿者 – ファイルのフィードバックを依頼されたユーザー。
- 表示者 – ファイルが共有されたが、ファイルへのアクセスが制限されている (表示のみ) ユーザー。
- 匿名の表示者 – 外部の表示リンクを介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、匿名の表示者は表示者と同じアクセス許可を持ちます。

共有フォルダのアクセス許可

共有フォルダに対して Amazon WorkDocs で定義されているアクセス許可を以下に示します。

- 表示 – 共有フォルダのコンテンツを表示します。
- サブフォルダの表示 – サブフォルダを表示します。
- 共有の表示 – フォルダを共有している他のユーザーを表示します。
- フォルダのダウンロード – フォルダをダウンロードします。
- サブフォルダの追加 – 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。
- 共有の取り消し – 最上位フォルダの共有を取り消します。
- サブフォルダの削除 – サブフォルダを削除します。
- 最上位フォルダの削除 – 最上位共有フォルダを削除します。

共有フォルダのアクセス許可

アクセス許可	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
表示	X	X	X	X
サブフォルダの表示	X	X	X	X
共有の表示	X	X	X	X
ダウンロード	X	X	X	X
サブフォルダの追加	X	X	X	
共有	X	X		
共有の取り消し	X	X		
サブフォルダの削除	X	X		
最上位フォルダの削除	X			

ファイルのアクセス許可

共有フォルダにないファイルに対して Amazon WorkDocs で定義されているアクセス許可を以下に示します。

- 表示 – ファイルを表示します。
- 削除 – ファイルを削除します。
- 注釈 – ファイルにフィードバックを追加できます。
- ファイルの共有 – ファイルを共有している他のユーザーを表示します。
- 注釈の表示 – 他のユーザーからのフィードバックを表示します。
- アクティビティの表示 – ファイルのアクティビティ履歴を表示します。
- ファイルのバージョン – ファイルの前のバージョンを表示します。

- 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。共有ファイルをダウンロードできるかどうかは、ファイルのプロパティで決まります。
- ダウンロードの禁止 – ファイルをダウンロードできないようにします。
- 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。
- 共有 – 他のユーザーとファイルを共有します。
- 共有の取り消し – ファイルの共有を取り消します。

共有フォルダダにないファイルのアクセス許可

アクセス許可	所有者/共同所有者	寄稿者	閲覧者	匿名の表示者
表示	X	X	X	X
共有の表示	X	X	X	X
ダウンロード	X	X	X	
注釈	X	X		
注釈の表示	X	X		
アクティビティの表示	X	X		
バージョンの表示	X	X		
アップロード	X	X		
削除	X			
ダウンロードの禁止	X			
共有	X			
共有の取り消し	X			

共有ファイルのアクセス許可

共有フォルダダのファイルに対して Amazon WorkDocs で定義されているアクセス許可を以下に示します。

- 表示 – 共有フォルダダのファイルを表示します。
- ファイルの共有 – ファイルを共有している他のユーザーを表示します。
- ダウンロード – ファイルをダウンロードします。
- 注釈 – ファイルにフィードバックを追加できます。
- 注釈の表示 – 他のユーザーからのフィードバックを表示します。
- アクティビティの表示 – ファイルのアクティビティ履歴を表示します。
- ファイルのバージョン – ファイルの前のバージョンを表示します。
- 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。
- 削除 – 共有フォルダダのファイルを削除します。
- ダウンロードの禁止 – ファイルをダウンロードできないようにします。これは、フォルダダのファイルに対するデフォルトのアクセス許可です。
- 共有 – 他のユーザーとファイルを共有します。
- 共有の取り消し – ファイルの共有を取り消します。

- プライベートコメント – 所有者/共同所有者は、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 (自分のコメントへの応答ではないコメントも含まれます)。

共有フォルダにあるファイルのアクセス許可

アクセス許可	フォルダ所有者/共同所有者	ファイル所有者*	フォルダ寄稿者	フォルダ表示者	匿名の表示者
表示	X	X	X	X	X
共有の表示	X	X	X	X	X
ダウンロード	X	X	X	X	
注釈	X	X	X		
注釈の表示	X	X	X		
アクティビティの表示	X	X	X		
バージョンの表示	X	X	X		
アップロード	X	X	X		
削除	X	X	X		
Rename	X	X			
ダウンロードの禁止	X	X			
共有	X	X			
共有の取り消し	X	X			
すべてのプライベートコメントを見る**	X	X			

*この場合、ファイルの所有者は、共有されたフォルダにファイルの元のバージョンを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、共有フォルダのすべてのファイルではなく、所有されたファイルのみに適用されます。

**ファイルの所有者/共同所有者はすべてのプライベートコメントを見ることができます。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。

共同編集の有効化

共同編集オプションは、[Admin control panel (管理コントロールパネル)] の [Online Editing Settings (オンライン編集の設定)] で有効にできます。

コンテンツ

Hancom ThinkFree の有効化

Amazon WorkDocs サイトで Hancom ThinkFree を有効にし、ユーザーが Amazon 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、共同で編集するようにできます。詳細については、「Hancom ThinkFree で編集する」を参照してください。

Hancom ThinkFree は、Amazon WorkDocs ユーザーは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 オンライン編集] の [変更] を選択します。
3. [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、[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 オンライン編集] の [変更] を選択します。
3. [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、[保存] を選択します。

[Office Online で開く] の有効化

Amazon WorkDocs サイトの [Office Online で開く] を有効にし、ユーザーが Amazon WorkDocs ウェブアプリケーションから Microsoft Office ファイルを共同で編集するようにできます。

[Office Online で開く] は、Microsoft Office 365 の Work または School アカウントと、Office Online で編集するライセンスを持っている Amazon WorkDocs ユーザーであれば、無料で使用できます。詳細については、「Office Online で開く」を参照してください。

[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. [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. [Office Online] で、[変更] を選択します。
3. [Enable Office Online (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

[Admin control panel (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. [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. [Office Online] で、[変更] を選択します。
3. [Enable Office Online (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。

Amazon WorkDocs へのファイルの移行

Amazon WorkDocs 管理者は Amazon WorkDocs 移行サービスを使用して複数のファイルやフォルダーを大規模に Amazon WorkDocs サイトに移行できます。Amazon WorkDocs 移行サービスは Amazon Simple Storage Service (Amazon S3) と連携します。これにより、部門ごとのファイル共有や、ホームドライブやユーザーファイルの共有を Amazon WorkDocs に移行できます。

このプロセス中に、Amazon 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、以下を行うためのアクセス権限を Amazon WorkDocs 移行サービスに付与する新しい IAM ロールを作成します。

- 指定された Amazon S3 バケットの読み取りおよびリスト。
- 指定された Amazon WorkDocs サイトの読み取りおよび書き込み。

次のタスクを完了して、ファイルとフォルダを Amazon WorkDocs に移行します。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。

- Amazon 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

Amazon WorkDocs サイトが Amazon 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、以下の要件に従う必要があります。

- Amazon 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、Amazon WorkDocs の予約されたユーザーロールです。
- Amazon 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 (p. 37)」および「ユーザーの編集 (p. 38)」を参照してください。

  Note

  ディレクトリ構造、ファイル名、ファイル内容は Amazon WorkDocs に移行しても維持されます。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: 移行の準備をする

移行の準備をするには

1. Amazon WorkDocs サイトで、[My Documents] の下に、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. 移行するファイルがそれぞれ 5 TB 未満であることを確認します。各ファイル名は 255 文字以下である必要があります。Amazon WorkDocs Drive では、フルディレクトリパスが 260 文字以下のファイルのみが表示されます。

   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、[Download report (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: ファイル名末尾の余分なスペース。
- 冒頭または末尾のピリオド–例: `.file`、`.file.ppt`、`.`、`..`、`file.`
- 冒頭または末尾のチルダ–例: `file.doc~`、`~file.doc`、`~$file.doc`
- **`.tmp`** で終わるファイル名–例: `file.tmp`
- 次の用語に大文字と小文字まで完全に一致するファイル名–`Microsoft User Data`、`Outlook files`、`Thumbs.db`、`Thumbnails`
- 以下のいずれかの文字を含むファイル名–`*` (アスタリスク)、`/` (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. AWS アカウントにファイルとフォルダをアップロードする新しい Amazon Simple Storage Service (Amazon S3) バケットを作成します。Amazon S3 バケットは Amazon WorkDocs と同じ AWS アカウントと AWS リージョンにある必要があります。詳細については、『Amazon Simple Storage Service 入門ガイド』の「Amazon Simple Storage Service の開始方法」を参照してください。
2. 前のステップで作成した Amazon S3 バケットにファイルをアップロードします。Amazon S3 バケットへのファイルとフォルダのアップロードには、AWS DataSync を使用することをお勧めします。DataSync では追跡、レポート作成、同期機能が追加で提供されます。詳細については、『AWS DataSync ユーザーガイド』の「AWS DataSync のしくみ」および「DataSync でアイデンティティベースのポリシー (IAM ポリシー) を使用する」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、Amazon WorkDocs 移行サービスを使用して移行をスケジューリングします。移行をスケジューリングすると、Amazon WorkDocs ユーザーアカウントの [Storage (ストレージ)] 設定が自動的に [Unlimited (無制限)] に変更されます。

Note

Amazon WorkDocs ストレージの制限を超えて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、「Amazon WorkDocs 料金表」を参照してください。

Amazon WorkDocs 移行サービスは移行に使用する AWS Identity and Access Management (IAM) ポリシーを提供します。このポリシーを使用して、Amazon WorkDocs 移行サービスが指定の Amazon S3 バケット

と Amazon WorkDocs サイトにアクセスするためのアクセス権限を付与する IAM ロールを作成します。また、Amazon SNS E 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ルされたとき、およびスケジュール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. Amazon WorkDocs コンソールで、[Apps (アプリ)]、[Migrations (移行)] を選択します。
   - 初めて Amazon WorkDocs 移行サービスに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指示されます。サブスクライブし、受信した E 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、[Create Migration (移行を作成)] を選択します。
3. [Source Type (ソースタイプ)] で、[Amazon S3] を選択します。
4. [Next] 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、提供される IAM ポリシーをコピーします。
6. 前のステップでコピーした IAM ポリシーを使用して、次のように新しい IAM ポリシーとロールと作成します。
   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、クリップボードにコピーしておいた IAM ポリシーに貼り付けます。
   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] 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。
      - 米国東部 (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、[Maximum CLI/API session duration (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. [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. Amazon WorkDocs 移行サービスに戻ります。[Data Source & Validation (データソースと検証)] の [Role ARN (ロール ARN)] に、前のステップでコピーした IAM ロールのロール ARN を貼り付けます。
8. [Bucket (バケット)] で、ファイルの移行元の Amazon S3 バケットを選択します。
9. [Next] を選択します。
10. [Select a destination WorkDocs Folder (宛先 WorkDocs フォルダを選択)] で、ファイルの移行先になる Amazon WorkDocs の宛先フォルダを選択します。
11. [Next] 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

Amazon WorkDocs 移行サービスのランディングページ内から、移行を追跡できます。Amazon WorkDocs サイトからランディングページにアクセスするには、[Apps (アプリ)]、[Migrations (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 [Cancel Migration (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 [Update (更新)] を選択します。移行が完了した後は、[Download report (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。

予定

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

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。

キャンセル済み

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 コンソールで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。

予定された移行が開始されると、Amazon WorkDocs ユーザーアカウントの [Storage (ストレージ)] 設定が自動的に [Unlimited (無制限)] に変更されます。移行後は、管理コントロールパネルからユーザーアカウントを編集して、[Storage (ストレージ)] 設定を変更できます。詳細については、「ユーザーの編集 (p. 38)」を参照してください。

Amazon WorkDocs に関するトラブルシューティング

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

問題点

特定の AWS リージョンの Amazon WorkDocs サイトを設定できない

新しい Amazon 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、「Amazon WorkDocs の開始方法 (p. 20)」で特定のユースケースのチュートリアルを参照してください。

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

新しい Amazon WorkDocs サイトを設定するときは、既存の仮想プライベートクラウド (VPC) を使用してディレクトリを作成します。Amazon 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 [Forgot password? (パスワードをお忘れですか?)] を選択して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] 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、[Share a link] 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 (p. 40)」を参照してください。

Amazon WorkDocs Drive または Amazon WorkDocs Companion アプリ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 Identity and Access Management (p. 4)」を参照してください。を複数のユーザーにデプロイする方法については、「Amazon WorkDocs Drive」を参照してください。複数のコンピュータへの Amazon WorkDocs Drive のデプロイ (p. 36)

オンライン編集が機能していない

Amazon WorkDocs Companion がインストールされていることを確認します。Amazon WorkDocs Companion をインストールする方法については、「Amazon WorkDocs のアプリと統合」を参照してください。

Amazon WorkDocs for Amazon Business の管理

Amazon WorkDocs for Amazon Business の管理者である場合は、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。

新しいユーザを Amazon WorkDocs for Amazon Business に招待するには

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. Amazon 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] を選択します。
4. [Add people] を選択します。
5. [Recipients] に、招待するユーザーの電子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] を選択します。

Amazon 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. Amazon 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] を選択します。
4. [Search users] で、ユーザーの名を入力し、**Enter** を押します。

Amazon 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. Amazon 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] を選択します。
4. [People] で、ユーザーの横にある [ロール] を選択して、ユーザーに割り当てます。

Amazon 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. Amazon 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] を選択します。
4. [People] で、省略記号 (...) をクリックします。
5. [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] を選択します。

ドキュメント履歴

以下の表は、Amazon WorkDocs 管理ガイド の 2018 年 2 月以降の重要な変更点をまとめたものです。このドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

update-history-change	update-history-description	update-history-date
Amazon WorkDocs for Amazon Business の管理 (p. 54)	Amazon WorkDocs for Amazon Business は、管理者によるユーザー管理をサポートします。詳細については、『Amazon WorkDocs 管理ガイド』の「Amazon WorkDocs for Amazon Business の管理」を参照してください。	March 26, 2020
Amazon WorkDocs へのファイルの移行 (p. 54)	Amazon WorkDocs 管理者は Amazon WorkDocs 移行サービスを使用して複数のファイルやフォルダーを大規模に Amazon WorkDocs サイトに移行できます。詳細については、『Amazon WorkDocs 管理ガイド』の「Amazon WorkDocs への移行」を参照してください。	August 8, 2019
IP 許可リストの設定 (p. 54)	IP 許可リストの設定は、IP アドレス範囲によって Amazon WorkDocs サイトへのアクセスをフィルター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 許可リストの設定」を参照してください。	October 22, 2018
Hancom ThinkFree (p. 54)	Hancom ThinkFree を使用できます。ユーザーは、Amazon WorkDocs ウェブアプリケーションから Microsoft Office ファイルを作成し、共同編集できます。詳細については、Amazon WorkDocs 管理ガイドの「Hancom ThinkFree の有効化」を参照してください。	June 21, 2018
Office Online で開く (p. 54)	[Office Online で開く] が使用可能になりました。ユーザーは、Amazon 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「[Office Online で開く] の有効化」を参照してください。	June 6, 2018

トラブルシューティング (p. 54)	トピックのトラブルシューティングを追加しました。詳細については、『Amazon WorkDocs 管理ガイド』の「Amazon 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。	May 23, 2018
リカバリ用ごみ箱の保持期間の変更 (p. 54)	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「リカバリ用ごみ箱の保持設定」を参照してください。	February 27, 2018

AWS の用語集

最新の AWS の用語については、『AWS General Reference』の「AWS の用語集」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。」