アマゾン WorkDocs

管理ガイド

アマゾン WorkDocs: 管理ガイド

Table of Contents

Amazon WorkDocsって何ですか

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、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 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、「」を参照してください。Amazon WorkDocs。

Amazon WorkDocs にアクセスする

管理者は、Amazon WorkDocs コンソールをクリックして Amazon WorkDocs サイトを作成し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、「WorkDocsサイト管理コントロールパネルからの Amazon の管理 (p. 27)」および「Amazon WorkDocs ユーザーを招待して管理します (p. 34)」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。Amazon WorkDocs コンソールや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。
- Amazon WorkDocs ドライブは、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アプリケーション。

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、およびサポートされているファイルの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

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してのみ料金が発生します。 詳細については、「」を参照してください。料金。

開始方法

Amazon WorkDocs の開始にあたっては、「」を参照してください。 WorkDocs アマゾンサイトの作成 (p. 20)。

アマゾンの前提条件 WorkDocs

新しい Amazon WorkDocs サイトのセットアップしたり、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。

AWS アカウントにサインアップする

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウント にサインアップするには

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環として、通話呼び出しを受け取り、電話のキーパッドを用いて検証コードを入力するように求められます。

   AWS アカウント にサインアップすると、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。セキュリティのベストプラクティスとして、管理ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS のサインアップ処理が完了すると、ユーザーに確認メールが送信されます。https://aws.amazon.com/ の [My Account] (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。

管理ユーザーを作成する

AWS アカウント にサインアップした後、日常的なタスクにルートユーザーを使用しないように、管理ユーザーを作成します。

AWS アカウントのルートユーザー をセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS Management Console 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 のルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理ユーザーを作成する

- 日常的な管理タスクのためには、AWS IAM Identity Center の管理ユーザーに管理アクセスを割り当てます。

  手順については、AWS IAM Identity Center ユーザーガイドの「開始方法」を参照してください。

管理ユーザーとしてサインインする

- IAM Identity Center ユーザーとしてサインインするには、IAM Identity Center 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。

アマゾンのセキュリティ WorkDocs

AWS では、クラウドのセキュリティが最優先事項です。AWS の顧客は、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から利点を得られます。

セキュリティは、AWS と顧客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 は、AWS クラウドで AWS の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負います。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 に適用されるコンプライアンスプログラムについてはWorkDocs、「AWSコンプライアンスプログラムによる対象サービス」を参照してください。
- クラウドのセキュリティ — AWS 使用するサービスによって責任が決まります。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、Amazon を使用する際に責任分担モデルを適用する方法を理解するのに役立ちますWorkDocs。

> **Note**
>
> WorkDocs特定の組織のユーザーは、ファイルへのリンクまたは招待状を送信することで、その組織外のユーザーと共同作業できます。サイトの共有リンク設定を確認し (p. 36)、会社の要件に最も適したオプションを選択してください。

以下のトピックでは、セキュリティとコンプライアンスの目標を満たすように Amazon WorkDocs を設定する方法を示しています。また、Amazon AWS WorkDocs リソースの監視と保護に役立つ他のサービスの使用方法についても学びます。

トピック

Amazon のアイデンティティとアクセス管理 WorkDocs

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するために役立つ AWS のサービス です。IAM 管理者は、Amazon リソースを使用するユーザーを認証 (サインイン) および許可 (アクセス権を持つ) できるユーザーを管理します。WorkDocsIAM は、追加費用なしで使用できる AWS のサービス です。

トピック

対象者

使用方法 AWS Identity and Access Management (IAM) 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 — Amazon WorkDocs のサービスを使用して業務を行う場合、管理者から必要な認証情報と権限が提供されます。作業に多くの Amazon WorkDocs 機能を使用するようになると、追加の権限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しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Amazon の機能にアクセスできない場合はWorkDocs、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 (p. 14)。

サービス管理者 — 会社で Amazon WorkDocs リソースを担当している場合は、Amazon へのフルアクセス権を持っているはずですWorkDocs。サービスユーザーがどの Amazon WorkDocs の機能やリソースにアクセスすべきかを決めるのはあなたの仕事です。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許可を変更する必要があります。このページの情報を確認して、IAM の基本概念を理解してください。会社が Amazon で IAM を使用する方法の詳細についてはWorkDocs、を参照してくださいAmazon と IAM WorkDocs の連携方法 (p. 9)。

IAM 管理者 — IAM 管理者であれば、Amazon へのアクセスを管理するポリシーを作成する方法について詳しく知りたいと思うかもしれません。WorkDocsIAM で使用できる Amazon WorkDocs ID ベースのポリシーの例については、を参照してください。Amazon WorkDocs アイデンティティベースのポリシーの例 (p. 11)

アイデンティティを使用した認証

認証とは、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。ユーザーは、AWS アカウントのルートユーザー として、または IAM ロールを引き受けることによって、認証済み (AWS にサインイン済み) である必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。 AWS IAM Identity Centerフェデレーティッドアイデンティティの例としては、(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 の認証情報などがあります。フェデレーティッドアイデンティティ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。フェデレーションを使用して AWS にアクセスする場合、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS Management Console または AWS アクセスポータルにサインインできます。AWS へのサインインの詳細については、AWS サインイン ユーザーガイドの「AWS アカウント にサインインする方法」を参照してください。

AWSプログラムでアクセスする場合、認証情報を使用してリクエストに暗号署名するための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 が提供されます。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。推奨される方法を使用して自分でリクエストに署名する方法の詳細については、IAM ユーザーガイドの「AWSAPI リクエストへの署名」を参照してください。

使用する認証方法を問わず、セキュリティ情報の提供を追加でリクエストされる場合もあります。例えば、AWS は、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「Multi-factor authentication」(多要素認証) および「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。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたは 1 つのアプリケーションに対して特定の許可を持つ AWS アカウント 内のアイデンティティです。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 ユーザーと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許可を指定できます。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許可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、ロールでは一時的な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 (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定の許可を持つ、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、特定のユーザーには関連付けられていません。ロールを切り替えることによって、AWS Management Console 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。

- フェデレーティッドユーザーアクセス – フェデレーティッドアイデンティティ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アイデンティティが認証されると、そのアイデンティティ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詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM アイデンティティセンターを使用する場合、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、アクセス許可セットを 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 Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー許可 - 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許可を一時的に 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を許可する主な方法は、ロールを使用することです。ただし、一部の 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 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。
- クロスサービスアクセス - 一部の AWS のサービス では、他の AWS のサービス の機能を使用します。例えば、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、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - プリンシパル許可 - IAM ユーザーまたはロールを使用して AWS でアクションを実行する場合、そのユーザーはプリンシパルと見なされます。ポリシーによって、プリンシパルに許可が付与されます。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。この場合、両方のアクションを実行するための許可が必要です。アク

ションにポリシーで追加の依存アクションが必要かどうかを確認するには、「Service Authorization Reference」(サービス認証リファレンス) をご参照ください。

- [Service role] (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 role] (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 - サービスにリンクされたロールは、AWS のサービス にリンクされたサービスロールの一種です。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、AWS アカウント 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 - EC2 インスタンスで実行され、AWS CLI または AWS API 要求を行っているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用できます。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的な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 ロールを使用して許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」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 AWS アイデンティティまたは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、アイデンティティ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。AWS 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、これらのポリシーを評価します。ポリシーでの許可により、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 ポリシー概要」を参照してください。

管理者は AWS JSON 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アクセス許可はありません。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アクセス許可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。このポリシーがあるユーザーは、AWS Management Console、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

アイデンティティベースポリシーは、IAM ユーザー、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、および条件を制御します。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」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ます。マネージドポリシーは、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。マネージドポリシーには、AWS マネージドポリシーとカスタマーマネージドポリシーがあります。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「マネージド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

リソースベースのポリシーは、リソースにアタッチする 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。ポリシーが添付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、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 AWS のサービス を含めることができます。

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 マネージド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

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コントロールします。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。

Simple Storage Service (Amazon S3)、AWS WAF、および Amazon VPC は、ACL をサポートするサービスの例です。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 では、その他の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) に付与できる許可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アクセス許可は、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、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) の最大許可を指定する JSON ポリシーです。AWS Organizations は、顧客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 と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」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許可される範囲は、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、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。

  Note

  Amazon は Slack WorkDocs 組織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許可を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が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 と IAM WorkDocs の連携方法

IAM を使用して Amazon へのアクセスを管理する前にWorkDocs、どの IAM 機能を Amazon で使用できるかを理解する必要があります。WorkDocsAmazon AWS やその他のサービスが IAM WorkDocs とどのように連携するかについての概要を知るには、IAM ユーザーガイドの「IAM AWS と連携するサービス」を参照してください。

トピック

- Amazon WorkDocs アイデンティティベースのポリシー (p. 9)
- Amazon WorkDocs リソースベースのポリシー (p. 10)
- Amazon WorkDocs タグに基づく認証 (p. 10)
- Amazon WorkDocs IAM ロール (p. 10)

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 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 User Guide」(IAM ユーザーガイド) の「IAM JSON policy elements reference」(IAM JSON ポリシー要素のリファレンス) をご参照ください。

アクション

管理者は AWS JSON 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、関連する 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許可を付与するポリシーで使用されます。

Amazon のポリシーアクションでは、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 オペレーションを実行する権限を誰かに付与するには、`workdocs:DescribeUsers`そのアクションをそのユーザーのポリシーに含めます。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。WorkDocsAmazon は、このサービスで実行できるタスクを説明する独自のアクションセットを定義しています。

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、次のようにカンマで区切ります。

```
"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することができます。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、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:*"
],
```

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

リソース

Amazon WorkDocs では、ポリシーでのリソース ARN の指定はサポートしていません。

条件キー

Amazon WorkDocs はサービス固有の条件キーを提供していませんが、一部のグローバル条件キーの使用は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

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

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 タグに基づく認証

Amazon WorkDocs では、リソースへのタグ付けやタグに基づくアクセス制御はサポートしていません。

Amazon WorkDocs IAM ロール

IAM ロールは AWS アカウント内のエンティティで、特定の許可を持っています。

Amazon での一時的な認証情報の使用 WorkDocs

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は、AWS STSAssumeRoleやなどの API オペレーションを呼び出すことで取得できますGetFederationToken。

Amazon 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ロール

サービスにリンクされたロールは、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することを許可します。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許可を表示できますが、編集することはできません。

Amazon 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。

サービスロール

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ロールを引き受けることが許可されます。このロールにより、サービスがユーザー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。サービスロールは、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 管理者が、このロールの許可を変更することができます。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

> 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 Amazon WorkDocs リソースを作成または変更する権限がありません。AWS Management Console、AWS CLI、または 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。

> 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

- ポリシーのベストプラクティス (p. 12)
- Amazon WorkDocs コンソールを使用する (p. 12)
- ユーザーが自分の許可を表示できるようにする (p. 13)

- 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 (p. 13)
- Amazon WorkDocs アイデンティティベースのポリシーのその他の例 (p. 14)

ポリシーのベストプラクティス

ID ベースのポリシーにより、アカウントの Amazon WorkDocs リソースを誰かが作成、アクセス、削除できるかどうかが決まります。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 マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの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のために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウント で使用できます。ユースケースに応じた AWS カスタマーマネージドポリシーを定義することで、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「AWS ジョブ機能の管理ポリシー」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ときは、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することができます。また、AWS のサービス などの特定の AWS CloudFormation を介して使用する場合、条件を使用して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。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (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、安全で機能的な許可を確保する - 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 Access Analyzer 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を作成できるようサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – AWS アカウント で IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。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 保護 API アクセスの設定」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。

Amazon WorkDocs コンソールを使用する

Amazon WorkDocs コンソールにアクセスするには、最低限の権限が必要です。これらの権限により、AWSアカウント内の Amazon WorkDocs リソースの詳細を一覧表示および表示できる必要があります。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 Amazon WorkDocs コンソールを使用できるようにするには、AWS以下の管理ポリシーもエンティティにアタッチしてください。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
- アマゾン EC2 FullAccess

これらのポリシーにより、ユーザーには Amazon WorkDocs リソース、AWSディレクトリサービスオペレーション、Amazon WorkDocs が正常に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権が付与されます。

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添付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": "*"
        }
    ]
}
```

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

AWSAmazonWorkDocsReadOnlyAccess以下の管理ポリシーでは、IAM ユーザーに Amazon WorkDocs リソースへの読み取り専用アクセス権を付与します。このポリシーにより、WorkDocsDescribeユーザーはすべてのAmazonオペレーションにアクセスできます。Amazon が VPC とサブネットのリストを取得するには、2 WorkDocs 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。AWS Directory Service ディレクトリに関する情報を取得するには、`DescribeDirectories` の AWS Directory Service 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ポリシーのその他の例

IAM 管理者は、IAM ロールまたはユーザーが Amazon WorkDocs API にアクセスできるようにする追加のポリシーを作成できます。詳細については、Amazon WorkDocs 開発者ガイドの「管理アプリケーションの認証とアクセス制御」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

以下の情報を使用して、Amazon と IAM WorkDocs を使用する際に発生する可能性のある一般的な問題の診断と修正に役立ててください。

トピック

Amazon でアクションを実行する権限がありません WorkDocs

AWS Management Console から、アクションを実行することが認可されてい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。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。

私には IAM を実行する権限がありません: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は、Amazon にロールを渡せるようにポリシーを更新する必要がありますWorkDocs。

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せずに、既存のロールをサービスに渡すことが許可されています。そのためには、サービスにロールを渡す許可が必要です。

次のエラー例は、という名前の IAM ユーザーがコンソールを使用して Amazon `marymajor` WorkDocs でアクションを実行しようとしたときに発生します。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アクセス許可が必要です。Mary 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、メアリー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 管理者に問い合わせてください。サインイン資格情報を提供した担当者が管理者です。

AWSアカウント外の人にも私の 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制御リスト (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 がこれらの機能をサポートしているかどうかについては、を参照してくださいいAmazon と IAM WorkDocs の連携方法 (p. 9)。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供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 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 にリソースへのアクセス権を提供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 への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でのロールとリソースベースのポリシーの使用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。

Amazon での口ギングとモニタリング WorkDocs

Amazon WorkDocs 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およびエクスポートできます。また、Amazon AWS CloudTrail WorkDocs コンソールからイベントをキャプチャするのにも使用できます。

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 (p. 15)
- Amazon WorkDocs API AWS CloudTrail 呼び出しの口ギングに使用する (p. 16)

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 Amazon WorkDocs Companion 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には、「Amazon 用アプリとインテグレーション」を参照してください。WorkDocs

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 — PC WorkDocsDownloadsのダウンロードフォルダーにあるフォルダー
   - 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。詳細については、Amazon WorkDocs ユーザーガイドの「アクティビティフィードを表示する」を参照してください。

Amazon WorkDocs API AWS CloudTrail 呼び出しの口ギングに使用する

AWS CloudTrail; を使用して Amazon WorkDocs API 呼び出しを口グに記録できます。CloudTrailAmazon のユーザー、ロール、AWSまたは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 WorkDocs。CloudTrailAmazon WorkDocs コンソールからの呼び出しや Amazon API へのコード呼び出しを含め、Amazon に対するすべての API WorkDocs 呼び出しをイベントとしてキャプチャします。WorkDocs

トレイルを作成すると、Amazon CloudTrail のイベントを含め、Amazon S3 バケットへのイベントの継続的な配信を有効にできますWorkDocs。証跡を作成しない場合でも、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することはできます。

CloudTrailによって収集される情報には、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、リクエスト日が含まれます。

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。

WorkDocsアマゾンの情報 CloudTrail

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 でアクティビティが発生するとWorkDocs、CloudTrailAWSそのアクティビティは他のサービスイベントとともにイベント履歴に記録されます。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 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 のイベントを含め、AWSアカウント内のイベントを継続的に記録するにはWorkDocs、トレイルを作成してください。トレイルを使用するとCloudTrail、Amazon S3 バケットにログファイルを配信できます。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、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、以下をご覧ください。

- 証跡を作成するための概要
- CloudTrail でサポートされるサービスと統合

- CloudTrail の Amazon SNS 通知の設定
- 「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」

Amazon WorkDocs のすべてのアクションは Amazon WorkDocs API CloudTrail リファレンスによって記録され、文書化されています。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。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 の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」を参照してください。

Amazon WorkDocs ログファイルエントリについて

[トレイル] は、指定した Simple Storage Service (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構成できます。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、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 は、コントロールプレーンからのものとデータプレーンからのものなど、CloudTrailさまざまなタイプの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 Amazon 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。これらはログに HIDDEN_DUE_TO _SECURITY_REASONS として表示されます。CloudTrailこれらはログに HIDDEN_DUE_TO _SECURITY_REASONS として表示されます。CloudTrail

次の例は、Amazon WorkDocs の 2 CloudTrail つの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で、2 番目のレコード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 のコンプライアンス検証 WorkDocs

AWS のサービス が特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスプログラムによる対象範囲内の AWS のサービス のサービス」をご覧いただき、関心のあるコンプライアンスプログラムを選択してください。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。

AWS Artifact 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。詳細については、「AWS Artifact におけるダウンロードレポート」を参照してください。

AWS のサービス を使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や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。AWS では、コンプライアンスに役立つ次のリソースを提供しています。

- セキュリティと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ステップを示します。
- 「アマゾン ウェブ サービスでの HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ」 – このホワイトペーパーは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法を説明しています。

Note

すべての AWS のサービス が HIPAA 適格であるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスのリソース– このワークブックおよびガイドのコレクションは、顧客の業界と拠点に適用されるものである場合があります。
- AWS Config デベロッパーガイドのルールでのリソースの評価 - AWS Config サービスでは、自社のプラクティス、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 のサービス は、AWS 内のセキュリティ状態の包括的なビューを提供します。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リストについては、「Security Hub のコントロールリファレンス」を参照してください。
- AWS Audit Manager - この AWS のサービス は AWS の使用状況を継続的に監査し、リスクの管理方法やコンプライアンスを業界スタンダードへの準拠を簡素化するために役立ちます。

アマゾンのレジリエンス WorkDocs

AWS の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ます。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立し隔離されたアベイラビリティーゾーンがあります。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、および拡張性が優れています。

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 のインフラストラクチャセキュリティ WorkDocs

WorkDocsマネージドサービスであるAmazonは、AWSグローバルなネットワークセキュリティ手順によって保護されています。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」と、AWS Architecture Center の「セキュリティ、アイデンティティ、および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公開されている API 呼び出しを使用して、WorkDocsネットワーク経由で Amazon にアクセスします。クライアントはトランスポート層セキュリティ (TLS) 1.2 をサポートしている必要があり、TLS 1.3 の使用をお勧めします。クライアントは、エフェメラル・ディフィー・ヘルマンやエリプティック・カーブ・エフェメラル・ディフィー・ヘルマンなど、パーフェクト・フォワード・シークレシー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、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 の開始方法 WorkDocs

Amazon WorkDocs は、サイトとそのドキュメントの組織情報を保存および管理するためにサイトを使用および管理します。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添付します。これを行うと、自動アクティベーションと呼ばれる Amazon WorkDocs の機能により、サイトへログインするために個別の認証情報を必要とせず、ファイルを共有および共同で作業することができ、サイトへログインするために個別の認証情報を必要とせず、ファイルを共有および共同で作業することができ、サイトへログインするために個別の認証情報を必要とせず、ファイルを共有および共同で作業することができ、サイトへログインするために個別の認証情報を必要とせず、ファイルを共有および共同で作業することができ、1 つのアクティベーションと呼ばれる Amazon の機能により、サイトへログインするために個別の 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「Amazon WorkDocs ユーザーを招待して管理します (p. 34)」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。
- Amazon WorkDocs が既存のAWSディレクトリと連携できるようにします。
- Amazon WorkDocs で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。このセクションの手順では、既存の Microsoft AD Directory を使用する方法について説明します。Microsoft AD ディレクトリの作成については、『AWSDirectory Service 管理ガイド』の「AWS Managed Microsoft AD」を参照してください。

内容

WorkDocs アマゾンサイトの作成

以下のセクションの手順では、新しい Amazon 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

Amazon サイトを作成するときは、Amazon WorkDocs サイトを作成する前に次のアイテムを持つことができます。

- AmazonAWS WorkDocs サイトを作成および管理するためのアカウント。ただし、ユーザーは、Amazon 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 WorkDocs。詳細については、「アマゾンの前提条件 WorkDocs (p. 2)」を参照してください。
- Simple AD を使用する予定の場合は、『AWS Directory Service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、AWS Managed Microsoft AD 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、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。このセクションの手順では、既存の Microsoft AD Directory を使用する方法について説明します。Microsoft AD ディレクトリの作成については、『AWSDirectory Service 管理ガイド』の「AWS Managed Microsoft AD」を参照してください。
- 姓名と E メールアドレスを含む管理者のプロファイル情報。

WorkDocs アマゾンサイトの作成

以下の手順に従って、Amazon WorkDocs サイトを数分で作成できます。

Amazon WorkDocs サイトを作成するには

1. https://console.aws.amazon.com/zocalo/ で Amazon 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 サイトの作成] で、[今すぐ始める] を選択します。

   -もしくは-

   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 サイトの作成] を選択します。

   次に実行される処理は、ディレクトリを持つ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、[ディレクトリの選択] ページが表示され、既存のディレクトリを選択したり、ディレクトリを作成したりできます。
   - ディレクトリがない場合は、「ディレクトリタイプのセットアップ」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. 上記のステップ 1 と 2 を繰り返します。

この時点で何をするかは、Simple AD を使用するか AD Connector を作成するかによって異なります。

Simple AD を使用するには

a. 「Simple AD」を選択し、「次へ」を選択します。

「Simple AD サイトの作成」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、苗字、名前を入力します。
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 サイトを作成」を選択します。

AD Connector ディレクトリを作成するには

a. [AD Connector] を選択し、[次へ] を選択します。

「AD Connector の作成」サイトページが表示されます。

b. [ディレクトリ詳細] 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 設定のオプションフィールドに入力します。
e. [AD Connector サイトの作成] を選択します。

Amazon WorkDocs は、以下のことを行います。

- 上記のステップ 4 で「代理で VPC をセットアップする」を選択した場合、Amazon が VPC WorkDocs を作成します。VPC のディレクトリには、ユーザーと Amazon WorkDocs サイトの情報が格納されます。
- Simple AD を使用した場合、Amazon WorkDocs はディレクトリユーザーを作成し、そのユーザーを Amazon 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、Amazon WorkDocs WorkDocs は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、Amazon WorkDocs WorkDocs 管理者のユーザー名を入力するように求められます。ユーザーは、ディレクトリのメンバーである必要があります。

Note

Amazon は、 WorkDocs 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 WorkDocs は、Amazon WorkDocs が登録されていのと同じディレクトリに参加しているコンピュータから、別途認証情報を入力することなく Amazon にアクセスすることをユーザーに許可します。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」(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。

Amazon WorkDocs 管理者がシングルサインオンを有効にした後、Amazon WorkDocs サイトのユーザーは、シングルサインオンを許可するためにウェブブラウザの設定を変更する必要がある場合もあります。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/AWS のディレクトリサービスコンソールを使用して、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。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、許可、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 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。AWS Managed AWS 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、『AWSDirectory 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

Amazon 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 Amazon 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 管理者の設定] 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ユーザー名を入力し、「管理者を設定」を選択します。

管理者を降格させるために、Amazon WorkDocs サイト管理コントロールパネルを使用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。

WorkDocs AWSコンソールから Amazon を管理する

Amazon 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。
- サイト管理者用コントロールパネル。すべての Amazon WorkDocs サイトの管理者が利用できます。

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、AWS コンソールが提供す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、「」を参照してくださいWorkDocsサイト管理コントロールパネルからの Amazon の管理 (p. 27)。

サイト管理者を設定する

管理者の場合は、ユーザーにサイトコントロールパネルへのアクセス権とサイトコントロールパネルが提供するアクションを与えることができます。

管理者を設定するには

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

   [WorkDocs サイトの管理] ページが開き、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、「管理者を設定」を選択します。

   [WorkDocs 管理者の設定] 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 E メールの再送信

招待 E メールはいつでも再送信できます。

招待 E メールを再送信するには

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

   [WorkDocs サイトの管理] ページが開き、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。

   緑色のバナーで成功を示すメッセージが表示されます。

多要素認証の管理

Amazon WorkDocs サイトを作成する場合、多要素認証を有効にすることができます。認証の詳細については、「多要素認証の有効化 (p. 23)」を参照してください。

サイト URL の設定

Note

のサイト作成プロセスに従った場合はAmazon の開始方法 WorkDocs (p. 20)、サイトの URL を入力しました。その結果、URL は 1 回しか設定できないため、Amazon WorkDocs では [サイト URL の設定] コマンドを使用できなくなります。Amazon をデプロイして Amazon WorkSpaces と統合する場合にのみ、以下の手順に従ってください WorkDocs。Amazon WorkSpaces 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、統合が完了したら URL を入力する必要があります。Amazon と Amazon の統合の詳細については WorkSpaces 、Amazon WorkDocs WorkSpaces ユーザーガイドの WorkDocs 「統合」を参照してください。

サイト URL を設定するには

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

   [WorkDocs サイトの管理] ページが開き、サイトのリストが表示されます。
3. Amazon と統合したサイトを選択します WorkSpaces。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 の設定」を選択します。

   [サイト URL の設定] 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 の設定」を選択します。
6. [WorkDocs サイトの管理] ページで [更新] を選択すると、新しい URL が表示されます。

通知の管理

Note

セキュリティを強化するには、可能な限り IAM ユーザーの代わりに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 CreateNotificationSubscriptionAPI を呼び出すことができます。これを使用して、 WorkDocs 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、Amazon WorkDocs 開発者ガイドの「IAM ユーザーまたはロールへの通知の設定」を参照してください。

通知の作成および削除が可能です。このステップでは、両方のタスクを実行する方法について説明します。

通知を作成するには

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

[WorkDocs サイトの管理] ページが開き、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。

[WorkDocs 管理者の設定] 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。

通知を削除するには

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

[WorkDocs サイトの管理] ページが開き、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、「管理者を設定」を選択します。

[WorkDocs 管理者の設定] 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。

サイトの削除

Amazon 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 Amazon WorkDocs コンソールを開きます。
2. ナビゲーションバーで、[Mites (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. 削除するサイトの横にあるボタンを選択し、[Delete (サイト)] を選択します。

[サイト URL の削除] ダイアログボックスが表示されます。

4. 必要に応じて、「ユーザーディレクトリも削除する」 を選択します。

> Important
>
> Amazon の独自のディレクトリを提供しない場合 WorkDocs、こちらで作成します。Amazon WorkDocs サイトを削除する場合、ディレクトリを削除するか、他の AWS アプリケーションに使用しない限り、こちらで作成したディレクトリに対して料金が請求されます。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 URL」ボックスにサイト 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。

WorkDocsサイト管理コントロールパネルからの Amazon の管理

Amazon WorkDocs サイトを管理するには、次のツールを使用します。

- サイト管理コントロールパネル。すべての Amazon WorkDocs サイトの管理者が使用でき、以下のトピックで説明しています。
- 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で提供され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の詳細については、「」を参照してくださいWorkDocs AWSコンソールから Amazon を管理する (p. 24)。

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. [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 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 (p. 47)」を参照してください。

[Storage] (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] (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 (p. 38)」をご参照ください。

IP 許可リスト

Amazon WorkDocs サイト管理者は IP 許可リスト設定を追加して、許可された範囲の IP アドレスへのサイトアクセスを制限できます。サイトあたり最大 32 個の [IP Allow List] (IP 許可リスト) の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. [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 Allow List] (IP 許可リスト) で、[Change] (変更) を選択します。
3. [CIDR 値の入力] で、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] (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 — ActiveDirectory シンプルなサイト

このトピックでは、Simple 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コネクタ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指定するには

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. [Admin] (管理) 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. [Security] (セキュリティ) まで下にスクロールし、 [Change] (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。次の表は、Simple ActiveDirectory サイトのセキュリティ設定の一覧です。

セッティング	説明
「共有可能なリンクの設定を選択」で、次のいずれかを選択します。	
サイト全体または一般公開の共有可能なリンクを許可しないでください	すべてのユーザーのリンク共有を無効にします。
サイト全体の共有リンクの作成はユーザーに許可するが、公開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。管理対象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リンクを作成できますが、公開共有リンクを作成できるのはパワーユーザーだけです	管理対象ユーザーはサイト全体のリンクを作成できますが、公開リンクを作成できるのはパワーユーザーだけです。公開リンクを使用すると、インターネット上の任意のユーザーともアクセスできます。
すべての管理対象ユーザーは、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	管理対象ユーザーは公開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。	
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が自動的にアクティブ化されるようにします。	ユーザーがサイトに初めてログインしたときに、自動的にユーザーをアクティブ化します。
「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。	
管理者のみが新しいユーザーを招待できます。	管理者のみが新しいユーザーを招待できます。
ユーザーは、ファイルやフォルダを共有することで、どこからでも新しいユーザーを招待できます。	ユーザーは、ファイルまたはフォルダーをユーザーと共有することで、新しいユーザーを招待できます。
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しいユーザーを招待できます。	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。
「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。	
ディレクトリの新規ユーザーは管理対象ユーザーになります (デフォルトではゲストユーザーです)	ディレクトリの新規ユーザーを管理対象ユーザーに自動的に変換します。

4. 終了したら、[変更を保存] を選択します。

セキュリティ — ActiveDirectory コネクタサイト

このトピックでは、ActiveDirectoryコネクタ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 を使用するサイトを管理している場合はActiveDirectory、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指定するには

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. [Admin] (管理) 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. [Security] (セキュリティ) まで下にスクロールし、 [Change] (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。次の表は、ActiveDirectoryコネクタサイトのセキュリティ設定の一覧と説明です。

セッティング	説明
「共有可能なリンクの設定を選択」で、次のいずれかを選択します。	
サイト全体または一般公開の共有可能なリンクを許可しないでください	選択すると、すべてのユーザーのリンク共有が無効になります。
サイト全体の共有リンクの作成はユーザーに許可するが、公開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。管理対象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リンクを作成できますが、公開共有リンクを作成できるのはパワーユーザーだけです	管理対象ユーザーはサイト全体のリンクを作成できますが、公開リンクを作成できるのはパワーユーザーだけです。公開リンクを使用すると、インターネット上の任意のユーザーともアクセスできます。
すべての管理対象ユーザーは、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	管理対象ユーザーは公開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。	
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が自動的にアクティブ化されるようにします。	ユーザーがサイトに初めてログインしたときに、自動的にユーザーをアクティブ化します。
「WorkDocsサイト内のディレクトリユーザーをアクティブ化できるのは誰に許可すべきか?」を参照してください。 で、以下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しいユーザーをアクティブ化できます。	管理者のみが新しい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することで、ディレクトリから新しいユーザーをアクティブ化できます。	ユーザーは、ディレクトリユーザーとファイルまたはフォルダーを共有することで、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の新規ユーザーをアクティブ化できます。	ユーザーは、特定のドメインのユーザーから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サイトに新規ユーザーを招待できるのは誰に許可すべきか？」をご覧ください。 で、以下のいずれかを選択します。	
[Share with external users (外部ユーザーとの共有)]	Enables administrators and users to invite new external users to your Amazon WorkDocs site.

セッティング	説明
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。	
Only administrators can invite new external users (管理者のみが新規外部ユーザーを招待可能)	管理者のみが外部ユーザーを招待することができます。
すべての管理対象ユーザーが新しいユーザーを招待できます	管理対象ユーザーが外部ユーザーを招待できるようにします。
パワーユーザーのみが新しい外部ユーザーを招待することができます。	パワーユーザーのみが新しい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、どちらかまたは両方のオプションを選択します。	
ディレクトリの新規ユーザーは管理対象ユーザーになります (デフォルトではゲストユーザーです)	ディレクトリの新規ユーザーを管理対象ユーザーに自動的に変換します。
[New external users will be Managed users (they are Guest users by default) (新しい外部ユーザーは管理対象ユーザーになります (デフォルトではゲストユーザーです))]	新しい外部ユーザーを管理対象ユーザーに自動的に変換します。

4. 終了したら、[変更を保存] を選択します。

ごみ箱の保持期間

ユーザーがファイルを削除すると、Amazon はそのファイルをユーザーのごみ箱に 30 WorkDocs 日間保管します。その後、Amazon はファイルを一時的なリカバリビンに 60 WorkDocs 日間移動し、その後完全に削除します。一時的なリカバリビンを表示できるのは管理者だけです。サイト全体のデータ保持ポリシーを変更することで、サイト管理者はリカバリビンの保持期間を最低 0 日、最大 365 日に変更できます。

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. リカバリ用ごみ箱にファイルを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、Amazon WorkDocs がユーザーファイルを完全に削除する前に、リカバリ用ごみ箱から復元することができます。

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、[Recover] (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 ユーザーを招待して管理します (p. 34)」を参照してください。

Amazon WorkDocs ドライブを複数のコンピュータ展開する

ドメインに参加しているマシンフリートの場合は、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 ドライブ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。

移動するときは、 Amazon WorkDocs ドライブで、すべての AWS IP アドレスのポート 443 に HTTPS アクセスが必要であることを忘れないでください。また、ターゲットシステムが Amazon WorkDocs ドライブのインストール要件を満たしていることを確認する必要もあります。詳細については、Amazon WorkDocs User GuideAmazon WorkDocsユーザーガイド(Amazon WorkDocsユーザーガイド)の「Installing Amazon WorkDocs Drive(Amazon WorkDocs ドライブのインストール)」を参照してください。

> **Note**
>
> GPO または SCCM を使用する場合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 ドライブクライアントをインストールします。

Amazon WorkDocs ドライブの MSI インストーラーは以下のオプション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 Amazon WorkDocs サイトの情報を自動入力します。例えば、 `SITEID=####`。
- **`DefaultDriveLetter`** - Amazon WorkDocs ドライブのマウントに使用するドライブ文字を自動入力します。たとえば、 `DefaultDriveLetter=W`。 ユーザーごとに異なるドライブ文字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 Amazon WorkDocs ドライブ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することができません。

次の例では、ユーザーインターフェイスや再起動なしで Amazon WorkDocs Drive をデプロイしています。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
```

Amazon WorkDocs ユーザーを招待して管理します

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、Amazonの自動アクティベーション機能により、 WorkDocs そのディレクトリ内のすべてのユーザーが管理対象ユーザーとして新しいサイトに追加されます。

では WorkDocs、管理対象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ありません。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 (p. 23)」を参照してください。

これらのタスクは、Amazon WorkDocs ウェブクライアントの管理コントロールパネルで行います。ただし、Amazon を初めて使用する場合は WorkDocs、管理タスクに取り掛かる前に、数分程度でさまざまなユーザーロールについて理解を深めてください。

内容

ユーザーロールの概要

Amazon WorkDocs では、以下のユーザーロールが定義さします。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 (p. 38)」を参照してください。

- Admin (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 (p. 23)」をご参照ください。
- パワーユーザー:管理者からの特別な権限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 — ActiveDirectory シンプルなサイト (p. 28) および「」を参照してくださいセキュリティ — ActiveDirectory コネクタサイト (p. 29)。
- ユーザー:Amazon WorkDocs サイトでファイルを保存したり、他のユーザーと共同作業したり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。

Amazon では、 WorkDocs 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

が割り当てられたユーザー WorkSpaces WorkSpace。

- すべてのAmazon WorkDocs 機能へアクセスできる
- 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 ストレージが割り当てられ、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Amazon WorkDocs 機能へアクセスできる
- 1 TB のデフォルトストレージ (pay-as-you-go追加ストレージは随時使用可能)
- 月額料金の対象

WorkDocs アマゾンユーザー

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

- すべてのAmazon WorkDocs 機能へアクセスできる
- 1 TB のデフォルトストレージ (pay-as-you-go追加ストレージは随時使用可能)
- 月額料金の対象

管理コントロールパネルを起動する

Amazon 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/オフを切り替えたり、ユーザーロールや設定の変更を行うことができます。

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. [Admin] (管理) 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。

   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、現在のユーザー、パワーユーザー、管理者など、誰が新しいユーザーを招待するかも決めることができます。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. [Admin] (管理) 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. [Security] (セキュリティ) まで下にスクロールし、 [Change] (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. [自動アクティベーション] で、[WorkDocs ディレクトリ内のすべてのユーザーがサイトに初めてログインしたときに自動的にアクティブ化されることを許可する] の横にあるチェックボックスをオフにします。

   [WorkDocs サイトのディレクトリユーザーのアクティベーションを許可するユーザー] でオプションが変わります。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。Amazon WorkDocs ユーザーは、リンクを共有することで、ファイルやフォルダーを共有できます。ファイルリンクは組織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. [Admin] (管理) 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. [Security] (セキュリティ) まで下にスクロールし、 [Change] (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. 「共有可能なリンクの設定を選択」で、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。

- ユーザーにサイト全体の共有可能なリンクの作成を許可するが、公開共有可能なリンクの作成は許可しない-リンクの共有をサイトメンバーのみに制限します。管理対象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で共有可能なリンクを作成できますが、公開共有リンクを作成できるのはパワーユーザーだけです。管理対象ユーザーはサイト全体のリンクを作成できますが、公開リンクを作成できるのはパワーユーザーだけです。公開リンクは、インターネット上の任意のユーザーへのアクセスが可能です。
- すべての管理対象ユーザーは、サイト全体で共有可能な公開リンクを作成できます。管理対象ユーザーは公開リンクを作成できます。

5. [Save Changes] (変更を保存する) を選択します。

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ることを覚えておいてください)、他のユーザーを招待する権限をユーザーに与えることができます。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. [Admin] (管理) 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. [Security] (セキュリティ) まで下にスクロールし、 [Change] (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. [WorkDocsサイト内の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、[外部ユーザーと共有] チェックボックスをオンにし、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て、[変更を保存] を選択します。

   -もしくは-

   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、[Save Changes] (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 — ActiveDirectory シ

ンプルなサイト (p. 28) およびセキュリティ — ActiveDirectory コネクタサイト (p. 29)「」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. [Admin] (管理) 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] (ユーザーを管理) で、[Invite Users] (ユーザーの招待) を選択します。
4. [Invite Users] (ユーザーの招待) 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、[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。

Amazon WorkDocs は、各受信者に招待メールを送信します。メールには、Amazon WorkDocs アカウントの作成方法に関するリンクと説明が含まれています。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. [Admin] (管理) 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] (ユーザーの編集) 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。

[First Name] (名) (クラウドディレクトリのみ)

ユーザーの名前。

[Last Name] (姓) (クラウドディレクトリのみ)

ユーザーの姓。

[Status] (ステータス)

ユーザーが [Active] (アクティブ) か [Inactive] (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 (p. 39)」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、 WorkSpaces WorkSpace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 (p. 34)」を参照してください。

[Storage] (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] (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 [Inactive] (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. [Admin] (管理) 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] (非アクティブ) を選択し、[Save Changes] (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、Amazon 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、そのユーザーのファイル、フォルダ、フィードバックは Amazon WorkDocs サイトから削除されません。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 (p. 39)」を参照してください。

保留中のユーザーの削除

保留状態の Simple AD、AWS管理対象の Microsoft ユーザー、AD Connector ユーザーを削除できます。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。

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、常に少なくとも 1 人いる必要があります。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 (p. 26)。

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、ユーザーをアクティブから非アクティブに切り替えて、 WorkDocs ユーザーがAmazonサイトにアクセスできないようにする必要があります。

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 (p. 39)」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. [Admin] (管理) 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] (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. [Save Changes (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、Amazon WorkDocs Companion をインストールする必要があります。Amazon WorkDocs コンパニオンをインストールするには、「Amazon 向けアプリとインテグレーション」を参照してください WorkDocs。

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. [Admin] (管理) 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
   - Admin
5. WorkDocs 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 (p. 34)」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。

Amazon は、WorkDocs権限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。システムは、ユーザーの役割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、Amazon 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。

- Amazon WorkDocs サイトのすべてのメンバーは、ファイルを検索し、表示し、コメントすることができます。
- このリンクがあれば、Amazon WorkDocs サイトのメンバーでない人でも、誰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、「WorkDocsサイト管理コントロールパネルからの Amazon の管理 (p. 27)」を参照してください。

招待による共有

招待による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、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。チームフォルダを作成して、作成したディレクトリグループと招待して共有することもできます。

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

詳細については、「WorkDocsサイト管理コントロールパネルからの Amazon の管理 (p. 27)」を参照してください。

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、余分なコストをかけずにファイルやフォルダを共有したり、外部ユーザーと共同作業することができます。受信者は Amazon WorkDocs サイトの有料ユーザーなる必要がなく、外部のユーザーとファイルやフォルダを共有することができます。外部共有を有効にすると、ユーザーは共有先となる外部ユーザーのメールアドレスを入力することで、表示者の共有アクセス権限を適切に設定することができます。外部ユーザーを追加すると、アクセス権限は表示者のみに制限され、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、Amazon にログインするために認証情報を入力しますWorkDocs。共有されるファイルやフォルダは [Shared with me] (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 (p. 34)」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、「WorkDocsサイト管理コントロールパネルからの Amazon の管理 (p. 27)」を参照してください。

許可

アマゾンWorkDocs権限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ーとファイルの権限を制御します。次のユーザーロールをフォルダーレベルで適用できます。

- フォルダーの所有者— フォルダまたはファイルの所有者。
- フォルダーの共同所有者— 所有者がフォルダまたはファイルの共同所有者として指定したユーザーまたはグループ。
- フォルダ投稿者— フォルダに無制限にアクセスできるユーザー。
- フォルダービューア— フォルダへのアクセスが制限されている (読み取り専用権限の) ユーザー。

個々のファイルレベルで次のユーザーロールを適用できます。

- オーナー— ファイルの所有者。
- 共同所有者— 所有者がファイルの共同所有者として指定したユーザーまたはグループ。
- 寄稿者— ファイルへのフィードバックを許可されているユーザー。

- ビューア— ファイルへのアクセスが制限されている (読み取り専用権限の) ユーザー。
- 匿名閲覧者— 組織外の未登録ユーザーで、外部閲覧リンクを使用して共有されたファイルを閲覧できるユーザー。特に明記されていない限り、匿名のビューワーはビューワー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

共有フォルダーのユーザーロールには次の権限が適用されます。

> Note
>
> フォルダーに適用される権限は、そのフォルダー内のサブフォルダーとファイルにも適用されます。

- [ビュー]— 共有フォルダーの内容を表示します。
- サブフォルダーを表示— サブフォルダーを表示します。
- シェアを表示— フォルダが共有されている他のユーザーを表示します。
- ダウンロードフォルダー— フォルダをダウンロードします。
- サブフォルダを追加— サブフォルダーを追加します。
- シェア— 最上位のフォルダーを他のユーザーと共有します。
- 共有を取り消す— 最上位フォルダーの共有を取り消します。
- サブフォルダを削除— サブフォルダーを削除します。
- 最上位フォルダーの削除— 最上位の共有フォルダーを削除します。

	表示	サブフォルダーを表示	シェアを表示	ダウンロードフォルダー	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	最上位フォルダーの削除
フォルダーの所有者	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダーの共同所有者	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダ投稿者	✓	✓	✓	✓	✓				
フォルダービューア	✓	✓	✓	✓					

共有フォルダ内のファイルに対する権限

共有フォルダー内のファイルのユーザーロールには、次の権限が適用されます。

- 注釈を付ける— フィードバックをファイルに追加します。

- [削除]— 共有フォルダー内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。
- ダウンロードを禁止— ファイルがダウンロードされないようにします。

  Note

  - このオプションを選択すると、ユーザーは[ビュー]権限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、共有フォルダーを開いてクリアしてくださいダウンロードを許可それらのユーザーにダウンロードさせたくない各ファイルの設定。
  - 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許可しない場合、寄稿者および閲覧者は Amazon でそのファイルを再生できませんWorkDocsWeb クライアント。
- シェア— 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。
- [ビュー]— 共有フォルダー内のファイルを表示します。
- シェアを表示— 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。
- バージョンを表示する— ファイルの以前のバージョンを表示する。
- バージョンを削除する— ファイルの 1 つまたは複数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。
- 非公開コメントをすべて表示— 所有者/共同所有者は、コメントへの返信でなくても、ドキュメントに対するすべての非公開コメントを表示できます。

	注釈	Delete	Rename (名前の変更)	アップロード	ダウンロード	ダウンロードを禁止	共有	共有を取り消す	表示	シェアを表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除する	バージョンを復元	プライベートコメントをすべて表示**
ファイル所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダー	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	注釈	Delete[2]	Rename (名前の変更)	アップロード	ダウンロード	ダウンロードを禁止	共有	共有を取り消す	表示	シェアを表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除する	バージョンを復元	プライベートコメントをすべて表示**
の所有者																
フォルダーの共同所有者	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
フォルダ投稿者	✓			✓	✓				✓	✓	✓	✓	✓			
フォルダービューア					✓				✓	✓						
匿名閲覧者									✓	✓						

*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。

共有フォルダにないファイルに対する権限

共有フォルダーに存在しないファイルのユーザーロールには、次の権限が適用されます。

- 注釈を付ける— フィードバックをファイルに追加します。
- [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。
- ダウンロードを禁止— ファイルがダウンロードされないようにします。

  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許可しない場合、寄稿者および閲覧者は Amazon でそのファイルを再生できませんWorkDocsWeb クライアント。
- シェア— 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。
- [ビュー]— ファイルを表示する。
- シェアを表示— 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。
- バージョンを表示する— ファイルの以前のバージョンを表示する。
- バージョンを削除する— ファイルの 1 つまたは複数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	Delete	Rename (名前の変更)	アップロード	ダウンロード	ダウンロードを禁止	共有	共有を取り消す	表示	シェアを表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除する	バージョンを復元
所有者	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
共同所有者	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[Contributor] (寄稿者)	✓			✓	✓				✓	✓	✓	✓	✓		
[Viewer] (表示者)					✓				✓	✓					

	注釈	Delete	Rename (名前の変更)	アップロード	ダウンロード	ダウンロードを禁止	共有	共有を取り消す	表示	シェアを表示	注釈を表示	アクティビティを表示	バージョンを表示	バージョンを削除する	バージョンを復元
匿名閲覧者									✓	✓					

共同編集の有効化

管理者コントロールパネルの「オンライン編集設定」セクションを使用して、共同編集オプションを有効にします。

内容

ハンコムの有効化 ThinkFree

Amazon WorkDocs サイトで Hancom ThinkFree を有効にすると、ユーザーは Amazon ウェブアプリケーションから Microsoft Office ファイルを作成して、共同で編集することができます。WorkDocs詳細については、「Hancom ThinkFree で編集」 をご参照ください。

Hancom ThinkFree は、Amazon WorkDocs ユーザーであれば、追加料金なしで利用することができます。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。

ハンコムを有効にするには ThinkFree

ThinkFree管理者コントロールパネルからHancom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。

ハンコムを無効にするには ThinkFree

ThinkFree管理者コントロールパネルからHancom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

Amazon WorkDocs サイトの [Office オンラインで開く] を有効にすると、ユーザーは Amazon WorkDocs ウェブアプリケーションから Microsoft Office ファイルを共同で編集できます。

Office Online で開く (Open with Office Online) は、Office Online で編集するためのライセンスを持つ Microsoft Office 365 職場アカウントまたは学校アカウントも持っている Amazon WorkDocs ユーザー向けに、追加費用なしでご利用いただけます。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. [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] (オフィスオンライン) で、[変更] (Change) を選択します。
3. [Enable Office Online] (Office Online の有効化) を選択し、[Save] (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] (オフィスオンライン) で、[Change] (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、[Save] (保存) を選択します。

ファイルをAmazon に移行する WorkDocs

Amazon WorkDocs の管理者は、Amazon WorkDocs Migration Service を使用して、Amazon WorkDocs サイトに複数のファイルやフォルダーの大規模な移行を行うことができます。Amazon WorkDocs Migration Service は、Amazon Simple Storage Service (Amazon S3) と連携しています。これにより、部門のファイル共有および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、Amazon WorkDocs Migration Service へのアクセス権を付与する新しい IAM ロールを作成し、以下を行います。

- 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 Amazon WorkDocs サイトの読み取りおよび書き込み。

以下のタスクを終了して、ファイルとフォルダーを 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 WorkSpaces サイトがフリートと同じディレクトリにセットアップされている場合は、これらの要件に従う必要があります。

- Amazon WorkDocs アカウントユーザー名に Admin (管理者) を使用しないでください。Admin (管理者) は Amazon WorkDocs で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、Upgraded WS User (アップグレードされた WS ユーザー) の必要があります。詳細については、ユーザーロールの概要 (p. 34) および ユーザーの編集 (p. 38) を参照してください。

> **Note**
>
> Amazon に移行する場合にディレクトリ構造、ファイル名、ファイル内容は保存されます WorkDocs。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: 移行のためのコンテンツの準備

コンテンツを移行準備するには

1. Amazon WorkDocs サイトの、[My Documents] (マイドキュメント) で、ファイルとフォルダの移行先のフォルダを作成します。

2. 次の点を確認します。

   - ソースフォルダーに含まれるファイルとサブフォルダーは 100,000 個までです。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 を超えることはありません。
   - 各ファイル名は 255 文字以下です。Amazon 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、[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。

- [Trailing spaces] (末尾のスペース)-例:ファイル名の末尾の余分なスペース。
- 最初または最後のピリオド — 例:`.file.file.ppt`、`.`、`..`、、`file.`
- 先頭または末尾のチルダ — 例:`file.doc~`、`~file.doc`、または`~$file.doc`
- 末尾が次のファイル名**`.tmp`** — 例:`file.tmp`
- 大文字と小文字が区別される次の用語に完全に一致するファイル名 —`Microsoft User DataOutlook files`、`Thumbs.db`、、または`Thumbnails`
- *(アスタリスク)、(フォワードスラッシュ)、/ (バックスラッシュ)、\ (バックスラッシュ)、: (小さい)、< (より大きい)、> (疑問符)、? (縦棒/パイプ)、|" (二重引用符) のいずれかを含むファイル名、または`\202E`(キャラクタコード 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 アカウントに、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 サイト同じ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 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ーを 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 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仕組み」と「アイデンティティベースのポリシー (IAM ポリシー) DataSync 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

手順の 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。

移行をスケジューリングする際に、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、「Amazon WorkDocs の料金」を参照してください。

Amazon WorkDocs 移行サービスは移行のために使用する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 移行サービスに、指定する Amazon S3 バケットおよび Amazon WorkDocs サイトへのアクセス権限を付与する新しい IAM 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. Amazon WorkDocs コンソールから、[アプリ]、[移行] を選択します。
   - Amazon 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指示されます。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、[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] (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. [Review policy] (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] (ポリシーを作成) 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、[Next: Review] (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。[Create role] (ロールの作成) を選択します。
   j. [Roles] (ロール) ページの [Role name] (ロール名) で、作成したロール名を選択します。
   k. [Summary] (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. [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. Amazon WorkDocs 移行サービスに戻ってください。[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. [Next] (次へ) を選択します。
10. [Select a destination WorkDocs Folder] (宛先 Folder) では、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] (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

Amazon 移行サービスのランディングページから、 WorkDocs 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、[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 [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。

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。

[Failed] (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. [Policies] (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. [Delete] (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。

スケジューリングされた移行が開始される際に、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] (ストレージ) 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 のトラブルシューティング WorkDocs問題点

以下の情報は、Amazon の問題のトラブルシューティングそ促進します WorkDocs。

問題点

自分の Amazon を設定できません WorkDocs 特定のサイトAWSリージョン

新しい Amazon を設定する場合 WorkDocs サイトで、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 の開始方法 WorkDocs (p. 20)」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。

Amazon のセットアップをしたい WorkDocs 既存の Amazon VPC のサイト

新しい Amazon をセットアップするとき WorkDocs サイトで、既存のVirtual Private Cloud (VPC) を使用してディレクトリを作成します。アマゾン WorkDocs は、このディレクトリを使用してユーザーを確認します。

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、[Share a link] (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 (p. 39)」を参照してください。

Amazon をデプロイする必要がある WorkDocs Drive or Amazon WorkDocs 複数ユーザーとの同伴者

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 のアイデンティティとアクセス管理 WorkDocs (p. 4)」を参照してください。Amazon のデプロイに関する具体的な情報について WorkDocs 複数ユーザーへのドライブについては、を参照してくださいAmazon WorkDocs ドライブを複数のコンピュータ展開する (p. 33)。

オンライン編集が機能していない

Amazon のアカウントを確認する WorkDocs コンパニオンがインストールされています。Amazon をインストールするには WorkDocs コンパニオン、「」Amazon 向けアプリとインテグレーション WorkDocs。

Amazon Business 用の Amazon WorkDocs の管理

Amazon WorkDocs for Amazon Business の管理者の場合は、 Amazon ビジネス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。

新しいユーザーを 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 のホームページで、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。

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 のホームページで、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。

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 のホームページで、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。

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 のホームページで、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

Amazon 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 WorkDocsで、次の IP アドレスとドメインを許可リストに追加します。そうすることで Amazon が有効になります WorkDocs とアマゾン WorkDocs に接続するドライブ WorkDocs のサービス。

- 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
- ゾカロ。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、を参照してください。AWSIP アドレスの範囲()AWS全般のサービス。

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お知らせをするために、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権限 (p. 58)	管理者は、バージョンの削除とバージョンの回復の権限を提供できるようになりました。権限は DeleteDocumentVersionAPI のリリースの一部です。	2022 年 7 月 29 日
WorkDocs アマゾン Backup (p. 58)	コンポーネントがサポートされなくなったため、Amazon WorkDocs Backup ドキュメントを Amazon WorkDocs 管理ガイドから削除しました。	2021 年 6 月 24 日
WorkDocs アマゾンビジネス向けアマゾンの管理 (p. 58)	Amazon WorkDocs ビジネスは、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 ビジネスでの Amazon Amazon for Amazon Migration Service を参照してください。	2020 年 3 月 26 日
Amazon へのファイルの移行 WorkDocs (p. 58)	Amazon WorkDocs の管理者は、Amazon WorkDocs Migration Service を使用して、Amazon WorkDocs サイトに複数のファイルやフォルダーの大規模な移行を行うことができます。詳細については、Amazon WorkDocs WorkDocs 管理ガイドの Amazon へのファイルの移行を参照してください。	2019 年 8 月 8 日
[IP allow list] (IP 許可リスト) の設定 (p. 58)	IP 許可リストの設定では、Amazon WorkDocs サイトへのアクセスをIPアドレス範囲でフィルタリングできます。詳細については、Amazon WorkDocs 管理ガイドの「IP 許可リスト設定」を参照してください。	2018 年 10 月 22 日
ハンコム ThinkFree (p. 58)	Hancom ThinkFree をお使いいただけます。ユーザーは、Amazon WorkDocs ウェブアプリケーションからの Microsoft Office ファイルを作成し、共同で編集することができま	2018 年 6 月 21 日

	す。詳細については、Amazon ThinkFree WorkDocs 管理ガイドの「Hancom を有効にする」を参照してください。	
[Open with Office Online] (p. 58) (Office Online で開く)	[Open with Office 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の Microsoft Office ファイルを共同で編集することができます。詳細については、Amazon WorkDocs 管理ガイドの Office Online で開くを有効にするを参照してください。	2018 年 6 月 6 日
[Troubleshooting] (p. 58) (トラブルシューティング)	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。	2018 年 5 月 23 日
リカバリービンの保存期間を変更 (p. 58)	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 管理ガイドの回復ビンの保存設定を参照してください。	2018 年 2 月 27 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 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。